Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
«Горно-Алтайский государственный университет»
Кафедра алгебры, геометрии
и методики преподавания математики

ТЕОРИЯ ЧИСЕЛ

Учебно-методический комплекс

Для студентов-бакалавров, обучающихся по направлению
010100 «Математика»

Горно-Алтайск
РИО Горно-Алтайского госуниверситета
2010

Печатается по решению редакционно-издательского совета
Горно-Алтайского государственного университета

УДК 511(075.8)
ББК 22.13я73
П88

Теория чисел: учебно-методический комплекс (для студентов-бакалавров, обучающихся по направлению 010100 «Математика»). — Горно-Алтайск: РИО ГАГУ, 2010. — 208 с.

Составители:
Пуркина В. Ф., к.п.н., доцент кафедры алгебры, геометрии и МПМ ГАГУ
Кайгородов Е. В., ст. лаборант кафедры алгебры, геометрии и МПМ ГАГУ

Рецензенты:
Крылов П. А., д.ф.-м.н., профессор, заведующий кафедрой алгебры ТГУ
Деев М. Е., к.ф.-м.н., доцент, заведующий кафедрой алгебры, геометрии и МПМ ГАГУ

Пособие содержит учебно-методические материалы по дисциплине «Теория чисел» для студентов дневного отделения физико-математического факультета II курса по направлению 010100 «Математика» и рассчитано на 1 семестр (четвертый). Дисциплина «Теория чисел» является общепрофессиональной дисциплиной федерального компонента ДН(М).Ф.18 для данного контингента студентов.

ОГЛАВЛЕНИЕ

1. БЛАГОДАРНОСТИ

Авторы выражают благодарность и признательность учителю информатики и информационно-коммуникационных технологий Шебалинской средней школы имени Л.В. Кокышева **Галине Александровне Буцаевой**, а также заместителю директора школы по информационным технологиям **Евгению Владимировичу Парошину** (выпускнику физико-математического факультета Горно-Алтайского государственного университета 2004 года) за ценные указания и замечания по стилистическому оформлению и содержанию учебно-методического комплекса «Теория чисел», а также за неоценимую техническую помощь при наборе и верстке сложных математических текстов в издательской системе LaTeX 2_ε.

Огромную благодарность приносим кандидату физико-математических наук, доценту кафедры математического анализа Горно-Алтайского государственного университета **Елене Александровне Раенко** за предоставленный образец учебно-методического комплекса, сверстанного в издательской системе LaTeX 2_ε, и советы практического содержания, которые оказались очень полезными при макетировании издания и подготовке его к печати.

Большую помощь в наборе текста настоящего учебно-методического комплекса оказали студенты физико-математического факультета Горно-Алтайского государственного университета (**Атачкин Андрей**, **Вырышев Павел**, **Артишева Наталья**, **Абрамова Елена** и многие другие). Всем им авторы также глубоко признательны и благодарны.

2. КВАЛИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА БАКАЛАВРА

Бакалавр математики подготовлен к выполнению деятельности в областях, использующих математические методы и компьютерные технологии; созданию и использованию математических моделей процессов и объектов; разработке эффективных математических методов решения задач естествознания, техники, экономики и управления; программно-управленческому обеспечению научно-исследовательской, проектно-конструкторской и эксплуатационно-управленческой деятельности.

Объектами профессиональной деятельности бакалавра математики являются научно-исследовательские центры, органы управления, образовательные учреждения, промышленное производство. Исходя из своих квалификационных возможностей, выпускник по направлению 010100 «Математика» может занимать должности: математик, инженер-программист (программист) и др. в соответствии с требованиями Квалификационного справочника должностей руководителей, бакалавров и других служащих, утвержденного постановлением Минтруда России от 21.08.98 №37.

3. НАБОР КОМПЕТЕНЦИЙ БАКАЛАВРА

Бакалавр математики отвечает следующим требованиям:

- Понимает возможности современных методов познания природы и владеет ими на уровне, необходимом для

решения задач, имеющих естественнонаучное содержание и возникающих при выполнении профессиональных функций.

- Умеет на научной основе организовывать свой труд.
- Способен в условиях развития науки и изменяющейся социальной практики к переоценке накопленного опыта, анализу своих возможностей, умеет приобретать новые знания, использовать другие формы обучения, включая самостоятельные и информационно-образовательные технологии.
- Понимает сущность и социальную значимость своей будущей профессии, основные проблемы дисциплин, определяющих конкретную область его деятельности, видит их взаимосвязь в целостной системе знаний.
- Способен поставить цель и сформулировать задачи, связанные с реализацией профессиональных функций, умеет использовать для их решения методы ранее изученных им наук.
- Способен к совершенствованию своей профессиональной деятельности в области математики.

После изучения курса «Теория чисел» студенты должны:

- овладеть основными методами современной теории чисел;
- приобрести опыт использования теоретико-числовых методов в процессе решения задач смежных математических дисциплин (алгебры, геометрии, математического анализа и т.д.);

- получить представление о роли теории чисел в системе математического знания и перспективах ее применения в естественных и гуманитарных науках.

4. РАБОЧАЯ ПРОГРАММА

Дисциплина «Теория чисел» ДН(М).Ф.18 является общепрофессиональной дисциплиной федерального компонента. Данный учебно-методический комплекс предназначен для студентов второго курса дневных отделений физико-математических факультетов по направлению 010100 «Математика» и рассчитано на один (четвертый) семестр.

4.1 Цели и задачи дисциплины

1. Познакомить студентов II курса с основными понятиями и методами современной теории чисел.
2. Научить применять их в процессе решения различных задач.
3. Раскрыть роль современной теории чисел в системе математического знания.
4. Сформировать у студентов теоретико-числовую составляющую математической культуры.

Студент должен **иметь представление**:

- О предмете и основных разделах теории чисел.
- О роли русских и советских математиков в развитии теории чисел.

- О влиянии теории чисел на развитие других разделов математики, применении теоретико-числовых результатов в математике и ее приложениях.
- Об алгебраических и трансцендентных числах.

Студент должен **знать**:

- Основные направления исследований и основные методы, используемые в теории чисел.
- О связях между разделами теории чисел.
- Основные понятия теорий делимости, систематических чисел, сравнений, цепных дробей.
- Основные числовые функции.
- Арифметические приложения теории сравнений.

Студент должен **уметь**:

- Решать основные типы задач по теории чисел:

  а) находить НОД и НОК двух и нескольких чисел, используя алгоритм Евклида;

  б) Находить значения функций $[x]$, $\{x\}$, $\tau(x)$, $\sigma(x)$, $\mu(x)$, $\varphi(x)$. Решать различные задачи по теории чисел, используя основные числовые функции;

  в) переводить числа из одной системы счисления в другую;

  г) представлять действительные числа в виде цепной дроби;

  д) решать сравнения первой, второй степени от одного неизвестного, показательные сравнения;

е) вычислять остатки при делении на данное число, проверять результаты арифметических действий, используя теорию сравнений.

4.2 Обязательные требования к минимуму содержания дисциплины

В результате изучения курса «Теория чисел» студенты должны овладеть следующим материалом:

Основные числовые функции и их свойства. Систематические числа, действия над ними. Цепные дроби. Разложение рационального числа в цепную дробь, вычисление подходящих дробей. Свойства подходящих дробей. Приближение действительных чисел подходящими дробями. Числовые сравнения и их свойства. Кольцо классов вычетов по простому модулю. Функция Эйлера. Теоремы Эйлера и Ферма. Сравнения и системы сравнений целой переменной. Равносильные сравнения степени n с одной переменной. Показатели чисел и классов вычетов по данному модулю. Теорема о числе первообразных корней по простому модулю. Индексы чисел и классов по данному модулю. Двучленные сравнения по простому модулю. Квадратичные вычеты и невычеты.

4.3 Распределение часов

Семестр	Учебные занятия						Контроль
	Общий объем	В том числе					
		аудиторные				Самост. работа	
		всего	из них				
			лекции	практич.	лабор.		
4	110	68	34	34	—	42	экз.

4.4. Технологическая карта учебного курса «Теория чисел»

Темы	Всего часов	Аудиторные занятия		Самост. занятия
		лекции	практ.	
Модуль №1				
Числовые функции	12	4	4	4
Модуль №2				
Систематические числа	14	4	4	6
Модуль №3				
Цепные дроби	18	6	4	8
Модуль №4				
Числовые сравнения	18	6	6	6
Модуль №5				
Сравнения с неизвестной величиной	30	8	10	12
Модуль №6				
Степенные вычеты	18	6	6	6
Итого	**110**	**34**	**34**	**42**
Форма итогового контроля		Экзамен		

4.5 Содержание дисциплины

Числовые функции

Понятие числовой функции. Мультипликативные функции. Числовые функции $[x]$, $\{x\}$, $\tau(x)$, $\sigma(x)$, $\mu(x)$ и их свойства. Распределение простых чисел и функция $\pi(x)$.

Систематические числа

Позиционные и непозиционные системы счисления. Переход от одной системы счисления к другой. Действия над систематическими числами в разных системах счисления.

Цепные дроби

Рациональные числа и цепные дроби. Подходящие дроби, их свойства. Бесконечные цепные дроби, квадратичные иррациональности.

Числовые сравнения

Отношение сравнимости по модулю, его свойства. Кольцо и поле классов вычетов. Функция Эйлера $\varphi(x)$. Теорема Эйлера и Ферма.

Сравнения с неизвестной величиной

Равносильность сравнений. Сравнение первой степени. Диофантовы уравнения, методы их решения. Системы сравнений, методы их решения. Системы сравнений, методы их решения. Сравнения высших степеней. Квадратичные вычеты и невычеты. Закон взаимности.

Степенные вычеты

Показатели, их свойства, первообразные корни и индексы.

4.5.1 Лекционный курс — 34 часа

Лекция №1

Числовые функции: $[x]$, $\{x\}$, $\tau(x)$, $\sigma(x)$, $\mu(x)$, $\pi(x)$.

Лекция №2

Позиционные и непозиционные системы счисления. Систематическая форма записи натурального числа.

Лекция №3

Переход от одной системы счисления к другой. Действия над систематическими числами.

Лекция №4

Цепные дроби. Подходящие дроби.

Лекция №5

Свойства подходящих дробей.

Лекция №6

Бесконечные цепные дроби, квадратичные иррациональности.

Лекция №7

Числовые сравнения, их свойства.

Лекция №8

Кольцо классов вычетов по данному модулю.

Лекция №9

Приведенная система вычетов, ее свойства. Функция Эйлера $\varphi(x)$.

Лекция №10

Тождество Гаусса. Теорема Эйлера и Ферма.

Лекция №11

Сравнения с переменной величиной. Равносильность сравнений.

Лекция №12

Сравнения первой степени с одной переменной. Диофантовы уравнения.

Лекция №13

Системы сравнений. Методы их решения.

Лекция №14

Сравнения высших степеней по простому модулю. Сравнения второй степени. Квадратичные вычеты и невычеты.

Лекция №15

Степенные вычеты. Показатели и их свойства.

Лекция №16

Первообразные корни по простому модулю. Теорема о числе первообразных корней.

Лекция №17

Индексы, их свойства, применение к решению сравнений.

4.5.2 Практические занятия — 34 часа

Практическое занятие №1

Числовые функции $\{x\}$, $[x]$, $\tau(x)$, $\sigma(x)$, $\mu(x)$. Распределение простых чисел.

Практическое занятие №2

Систематические числа и действия над ними.

Практическое занятие №3

Контрольная работа по темам «Числовые функции» и «Систематические числа».

Практическое занятие №4

Цепные дроби и рациональные числа. Подходящие дроби и их свойства.

Практическое занятие №5

Квадратичные иррациональности и бесконечные цепные дроби.

Практическое занятие №6

Контрольная работа по теме «Цепные дроби».

Практическое занятие №7

Числовые сравнения. Кольцо классов вычетов по составному модулю и поле по простому модулю.

Практическое занятие №8

Функция Эйлера и ее свойства.

Практическое занятие №9

Функция Эйлера. Теорема Эйлера и Ферма.

Практическое занятие №10

Контрольная работа по теме «Числовые сравнения».

Практическое занятие №11

Сравнения с неизвестной величиной. Сравнения первой степени.

Практическое занятие №12

Диофантовы уравнения, методы их решения.

Практическое занятие №13

Системы сравнений, методы их решения.

Практическое занятие №14

Сравнения высших степеней. Квадратичные вычеты и невычеты.

Практическое занятие №15

Показатели и их свойства.

Практическое занятие №16

Первообразные корни по простому модулю, алгоритм нахождения первообразных корней. Индексы. Решение сравнений с помощью индексов.

Практическое занятие №17

Контрольная работа по темам «Сравнения с неизвестной величиной» и «Степенные вычеты».

4.5.3 Самостоятельная работа — 42 часа

Самостоятельная работа студентов рассматривается как вид учебного труда, позволяющий целенаправленно формировать и развивать самостоятельность студента как личностное качество при выполнении различных видов заданий и проработке дополнительного учебного материала.

Для успешного выполнения расчетных заданий, написания рефератов и подготовки к коллоквиуму, помимо материалов лекционных и практических занятий, необходимо

использовать основную и дополнительную литературу, указанную на стр. 204 настоящего пособия. Кроме того, студентам необходимо выполнить индивидуальные задания по основным темам курса, оценки за которые учитываются при выставлении оценок на экзамене.

№	Темы	Кол-во часов	Формы отчетности	Сроки
1	Асимптотический закон распределения простых чисел	4	Реферат	февраль
2	История развития теории чисел	6	Реферат	февраль
3	Наилучшие приближения действительных чисел	8	Коллоквиум	март
4	Различные методы решения сравнений первой степени	6	Расчетное задание	март
5	Сравнения n-ой степени по составному модулю. Символ Лежандра и Якоби	12	Коллоквиум	апрель
6	Первообразные корни по модулям p и $2p$. Алгебраические и трансцендентные числа	6	Реферат	май

4.5.4 Темы курсовых работ

1. История становления и развития теории чисел.
2. П. Л. Чебышев, его вклад в теорию чисел.
3. Распределение простых чисел в натуральном ряду и в арифметических прогрессиях.
4. Квадратичные иррациональности и цепные дроби.
5. Методы решения сравнений n-ой степени.
6. Закон взаимности квадратичных вычетов.
7. Сравнения высших степеней по составному модулю.
8. Алгебраические и трансцендентные числа.
9. Диофантовы уравнения.

5. ВОПРОСЫ К ЭКЗАМЕНУ

1. Числовые функции $\{x\}$, $[x]$, $\tau(x)$, $\sigma(x)$, $\mu(x)$.
2. Функция $\pi(x)$ и неравенство Чебышева.
3. Позиционные и непозиционные системы счисления. Систематическая запись натурального числа.
4. Переход от одной системы счисления к другой. Два способа.
5. Цепные дроби. Подходящие дроби, их свойства.
6. Вывод рекуррентных формул:

$$P_k = P_{k-1}q_k + P_{k-2}; \qquad Q_k = Q_{k-1}q_k + Q_{k-2}.$$

7. Вывод формулы:

$$P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k.$$

8. Доказательство неравенства:

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_kQ_{k+1}} < \frac{1}{Q_k^2}.$$

9. Числовые сравнения, их свойства.

10. Кольцо классов вычетов по данному модулю.

11. Полная и приведенная система вычетов, их свойства.

12. Функция Эйлера, её свойства, формула для вычисления.

13. Теорема Эйлера и Ферма, их применение к решению задач.

14. Сравнения с переменной величиной, теоремы о равносильности сравнений.

15. Сравнения первой степени с одной переменной. Случай, когда $(a,\ m) = 1$.

16. Сравнения первой степени с одной переменной. Случай, когда $(a,\ m) = d$ и $b \vdots d$.

17. Сравнения первой степени с одной переменной. Случай, когда $(a,\ m) = d$ и $b \not\vdots d$.

18. Диофантовы уравнения. Методы их решения.

19. Системы сравнений первой степени с одной переменной.

20. Сравнения высших степеней по простому модулю. Методы их решения.

21. Сравнение второй степени по простому модулю. Теорема о числе квадратных вычетов и невычетов.

22. Критерий Эйлера о квадратных вычетах.

23. Степенные вычеты. Порядок класса вычетов. Свойства показателей.

24. Теорема о числе классов вычетов, принадлежащих данному показателю.

25. Первообразные корни. Теорема о числе первообразных корней по простому модулю. Алгоритм их вычисления.

26. Индексы, их свойства.

27. Применение индексов к решению сравнений.

6. ЛЕКЦИИ ПО ТЕОРИИ ЧИСЕЛ

Предварительные сведения

В процессе изучения основных разделов теории чисел нам потребуются некоторые теоретические сведения из курса «Теория делимости в кольце целых чисел», поэтому повторите ранее изученный материал («Алгебра», часть 1). Не умаляя общности, приведем ниже ряд утверждений, касающихся делимости целых чисел, а также взаимно простых чисел и их свойств.

У т в е р ж д е н и е 1. *Если* $a \vdots c$ *и* $b \vdots c$, *то* $(a+b) \vdots c$.

Д о к а з а т е л ь с т в о. Так как $a \vdots c$ и, кроме того, $b \vdots c$, то $\exists q,\ t \in \mathbb{Z} \mid a = cq$ и $b = ct$. Но тогда $a + b = cq + ct = c(q + t)$. Поскольку $q + t$ — целое число, то $a + b$ делится на c. Утверждение доказано.

Утверждение 2. *Если числа a и b взаимно просты и $a \vdots a_1$, а $b \vdots b_1$, то числа a_1 и b_1 взаимно просты.*

Доказательство. Так как $(a,\ b) = 1$, то $\exists x,\ y \in \in \mathbb{Z} \mid ax + by = 1$ (см. «Алгебра», часть 1). Но по условию $a = a_1 q$, $b = b_1 t$, а потому $a_1(qx) + b_1(ty) = 1$. Это равенство показывает, что a_1 и b_1 взаимно просты. Утверждение доказано.

Утверждение 3. *Если произведение двух чисел $a \cdot b$ делится на c, и a взаимно просто с c, то b делится на c.*

Доказательство. Так как $(a,\ c) = 1$, то $\exists x,\ y \in \in \mathbb{Z} \mid ax + cy = 1$. Умножая обе части этого равенства на b, получим: $abx + cby = b$. По условию $ab \vdots c$, следовательно, левая часть последнего равенства (в силу утверждения 1) делится на c. Но тогда и правая часть тоже делится на c, т.е. $b \vdots c$. Утверждение доказано.

Утверждение 4. *Если два числа a и b взаимно просты с третьим числом c, то и их произведение взаимно просто с c. Верно и обратное.*

Доказательство. Доказательство проведем от противного. Пусть $(ab,\ c) = d > 1$. Тогда $c \vdots d$. Так как по условию $(a,\ c) = 1$, то по утверждению 2 и $(a,\ d) = 1$. Поскольку $ab \vdots d$ и $(a,\ d) = 1$, то по утверждению 3 $b \vdots d$. Значит, d является общим делителем чисел b и c, что противоречит условию о том, что эти числа взаимно просты. Полученное противоречие доказывает, что $(ab,\ c) = 1$.

Докажем теперь обратное утверждение. Пусть произведение ab взаимно просто с c. Нужно показать, что тогда числа a и b по отдельности взаимно просты с c. Предположим противное, т.е. пусть хотя бы одно из этих чи-

сел не взаимно просто с c, например, $(a,\ c) = l > 1 \Rightarrow$ $\Rightarrow (a \vdots l)\ \&\ (c \vdots l)$. Но тогда и $ab \vdots l$. Имеем: l — общий делитель чисел ab и c, что невозможно, так как $(ab,\ c) = 1$. Полученное противоречие доказывает, что $(a,\ c) = 1$ и $(b,\ c) = 1$. Утверждение полностью доказано.

У т в е р ж д е н и е 4′. *Если каждое из чисел* $a_1,\ a_2,\ \ldots a_m$ *взаимно просто с каждым из чисел* $b_1,\ b_2,\ \ldots b_n$, *то и произведение* $a_1 \cdot a_2 \cdot \ldots \cdot a_m$ *взаимно просто с произведением* $b_1 \cdot b_2 \cdot \ldots \cdot b_n$.

Д о к а з а т е л ь с т в о. Имеем: $(a_i,\ b_k) = 1$, где $i = 1,\ 2,\ \ldots,\ m,\ k = 1,\ 2,\ \ldots,\ n$. Тогда в силу утверждения 4 получим: $(a_1 \cdot a_2,\ b_k) = 1$, $(a_1 \cdot a_2 \cdot a_3,\ b_k) = 1$ и т.д. В конце концов придем к тому, что $(a_1 \cdot a_2 \cdot \ldots \cdot a_m,\ b_k) = 1$, т.е. произведение $a_1 \cdot a_2 \cdot \ldots \cdot a_m = A$ взаимно просто с b_k $(k = 1,\ 2,\ \ldots,\ n)$. Рассуждая аналогично, будем иметь $(A,\ b_1) = (A,\ b_1 \cdot b_2) = \ldots = (A,\ b_1 \cdot b_2 \cdot \ldots \cdot b_n) = 1$, т.е. $a_1 \cdot a_2 \cdot \ldots \cdot a_m$ взаимно просто с $b_1 \cdot b_2 \cdot \ldots \cdot b_n$. Утверждение доказано.

У т в е р ж д е н и е 5. *Если числа* a *и* b *взаимно просты, то любые их натуральные степени — взаимно простые числа.*

Д о к а з а т е л ь с т в о. Положив в утверждении 4′ $a_1 = a_2 = \ldots = a_m = a$ и $b_1 = b_2 = \ldots = b_n = b$, получим: $(a^m,\ b^n) = 1$. Утверждение доказано.

У т в е р ж д е н и е 6. *Пусть* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ — *каноническое разложение натурального числа* n. *Для того, чтобы натуральное число* d *являлось делителем числа* n, *необходимо и достаточно, чтобы простые делители числа* d *входили в разложение на множители числа* n *с показателями степени не меньшими тех, в каких они входят в*

разложении числа d:

$d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, причем $0 \leqslant \beta_i \leqslant \alpha_i$ $(i = 1,\ 2,\ \ldots,\ k)$.

Доказательство.

Необходимость. Пусть $n \vdots d \Rightarrow n = dq,\ q \in \mathbb{Z}$. Если бы делитель d имел в своем разложении простой множитель, какого нет в разложении n, или в разложении d был бы простой множитель в степени большей, чем он входит в разложение n, то тогда для одного и того же числа были бы два различных разложения n и dq на простые множители, что противоречит основной теореме арифметики (см. «Алгебра», часть 1). Следовательно, все простые делители числа d входят в разложение на множители числа n с показателями β_i, где $0 \leqslant \beta_i \leqslant \alpha_i$. Поэтому все делители числа n имеют вид $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, где $0 \leqslant \beta_i \leqslant \alpha_i$.

Достаточность. Если $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ и выполнены условия $0 \leqslant \beta_i \leqslant \alpha_i$, то будет иметь место равенство $n = dq$, где за число q следует взять произведение всех тех простых множителей, которые входят в n и не входят в d, и умножить его на общие для n и d простые делители, взяв их с показателями, равными разностям показателей, с которыми они входят в число n и число d. Таким образом, выражения вида $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, где $0 \leqslant \beta_i \leqslant \alpha_i$, будут являться делителями числа n. Утверждение доказано.

Глава I. Числовые функции

§1. Понятие числовой функции

1. Определение числовой функции.

О п р е д е л е н и е 1. Функция f называется *числовой*, если она определена для любого натурального числа x.

Согласно этому определению многие функции из курса математического анализа являются числовыми, например, e^x, $\sin x$, $\log_a x$ и другие. В теории чисел рассматриваются такие числовые функции, которые:

а) либо определены только при натуральных значениях аргумента;

б) либо функции, для которых натуральные значения являются характерными точками, определяющими величину функции в других точках.

2. Мультипликативные функции и их свойства.

О п р е д е л е н и е 2. Функция $f(x)$ называется *мультипликативной*, если она удовлетворяет следующим требованиям:

1). $\forall a \in \mathbb{N}\ f(a) \neq 0$;

2). $\forall a, b \in \mathbb{N} \mid (a, b) = 1 \rightarrow f(a \cdot b) = f(a) \cdot f(b)$.

Т е о р е м а 1. *Если $f(x)$ мультипликативна, то* $f(1) = 1$.

Д о к а з а т е л ь с т в о. Имеем: $\forall x \in \mathbb{N}\ f(x)$ мультипликативна, причем

$$f(x) = f(x \cdot 1) = f(x) \cdot f(1) \rightarrow f(1) = 1,$$

что и требовалось доказать.

Т е о р е м а 2. *Пусть дана мультипликативная функция $f(x)$ и натуральные числа $a_1, a_2, \ldots a_s$ попарно*

взаимно просты, т.е. $\forall i \neq j \ (a_i, a_j) = 1$. *Тогда*

$$f(a_1 \cdot a_2 \cdot \ldots \cdot a_s) = f(a_1) \cdot f(a_2) \cdot \ldots \cdot f(a_s).$$

Доказательство. Доказательство проведем методом математической индукции по числу сомножителей:

1) Пусть $s = 2$. Тогда

$$f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2).$$

Это равенство верно в силу определения мультипликативной функции.

2) Предположим, что для $s = k - 1$ справедливо равенство

$$f(a_1 \cdot a_2 \cdot \ldots \cdot a_{k-1}) = f(a_1) \cdot f(a_2) \cdot \ldots f(a_{k-1}).$$

3) Пусть $s = k$. Тогда

$$f(a_1 \cdot a_2 \cdot \ldots \cdot a_{k-1} \cdot a_k) = f(A \cdot a_k),$$

где $A = a_1 \cdot a_2 \cdot \ldots \cdot a_{k-1} \in \mathbb{N}$.

Но числа A и a_k в силу утверждения $4'$ взаимно просты. Поэтому будет верно равенство:

$$f(A \cdot a_k) = f(A) \cdot f(a_k) = f(a_1) \cdot f(a_2) \cdot \ldots \cdot f(a_{k-1}) \cdot f(a_k).$$

Теорема доказана.

Теорема 3. *Если каноническая запись числа* n *имеет вид* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, *а* $f(n)$ — *мультипликативная функция, то*

$$f(n) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdot \ldots \cdot f(p_k^{\alpha_k}).$$

Доказательство. Справедливость теоремы вытекает из того, что числа $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, $\ldots$, $p_k^{\alpha_k}$ попарно взаимно просты (в силу утверждения 5), и из теоремы 2.

С в о й с т в о. *Произведение мультипликативных функций есть мультипликативная функция.*

Д о к а з а т е л ь с т в о. Пусть даны две мультипликативные функции $f_1(x)$ и $f_2(x)$. Покажем, что функция $f(x) = f_1(x) \cdot f_2(x)$ будет также мультипликативной. Действительно,

1. $f(1) = f_1(1) \cdot f_2(1) = 1 \cdot 1 = 1$;
2. $\forall a, b \in \mathbb{N} \mid (a, b) = 1$, имеем:

$$f(a \cdot b) = f_1(a \cdot b) \cdot f_2(a \cdot b) = f_1(a) \cdot f_1(b) \cdot f_2(a) \cdot f_2(b) =$$
$$= f_1(a) \cdot f_2(a) \cdot f_1(b) \cdot f_2(b) = f(a) \cdot f(b).$$

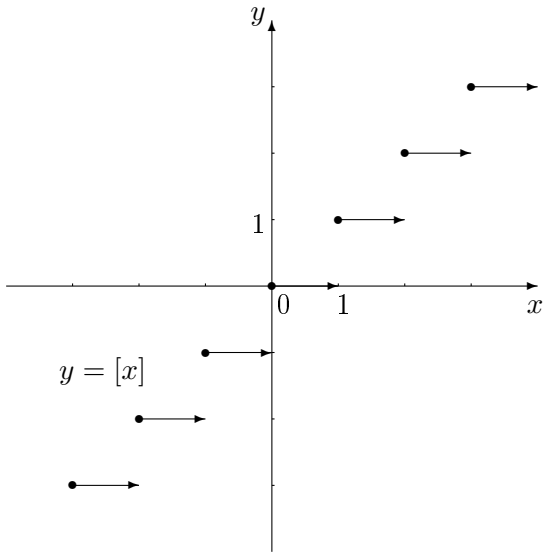
Свойство доказано.

§2. Примеры числовых функций

1. Целая часть действительного числа $[x]$.

О п р е д е л е н и е 3. *Целой частью* действительного числа x называется наибольшее целое число, не превосходящее x, т.е. $[x] \leqslant x < [x] + 1$. Обозначение: $f(x) = [x]$.

График функции $y = [x]$ имеет вид:



З а д а ч а 1. Вычислить: а) [3,12]; б) [0,5]; в)[−1,5].

Р е ш е н и е. а) $[3{,}12] = 3$; б) $[0{,}5] = 0$; в) $[-1{,}5] = -2$.

Рассмотрим применение функции $y = [x]$ для решения некоторых задач.

З а д а ч а 2. Сколько положительных чисел, не превосходящих n, делятся на m?

Р е ш е н и е. Разделим n на m с остатком: $n = mq + r$, где $0 \leqslant r < m$. Числа, кратные m, суть: m, $2m$, $\ldots$, qm. Их количество будет равно q. Но, с другой стороны, из $n = mq + r$ следует, что $\dfrac{n}{m} = q + \dfrac{r}{m}$. Так как $0 \leqslant \dfrac{r}{m} < 1$, то $\left[\dfrac{n}{m}\right]$ тоже равно q.

Функция $y = [x]$ позволяет вычислить показатель, с которым данное простое число p входит в произведение $n!$

Т е о р е м а 4. *Показатель, с которым простое число p входит в разложение $n!$, равен*

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots + 0.$$

Д о к а з а т е л ь с т в о. Очевидно, ряд

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

обрывается на том месте k, на котором p^k превзойдет n.

Понятно, что среди чисел 1, 2, $\ldots$, n есть $\left[\dfrac{n}{p}\right]$ чисел, кратных p, $\left[\dfrac{n}{p^2}\right]$ — кратных p^2, $\ldots$, $\left[\dfrac{n}{p^k}\right]$ — кратных p^k.

Каждое число 1, 2, $\ldots$, n, кратное p, но не кратное p^2, дает в произведении $n! = 1 \cdot 2 \cdot \ldots \cdot n$ один простой множитель, равный p. Числа, кратные p^2, но при этом не кратные p^3, дают два таких множителя и т.д. Поэтому, общее число

простых множителей, равных p, в каноническом разложении $n!$ таково:

$$\alpha = \left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right] + 2\left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right) +$$

$$+3\left(\left[\frac{n}{p^3}\right] - \left[\frac{n}{p^4}\right]\right) + \ldots + k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right).$$

Раскрывая скобки и приводя подобные члены, получим, что

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] \ldots + \left[\frac{n}{p^k}\right] + 0.$$

Теорема доказана.

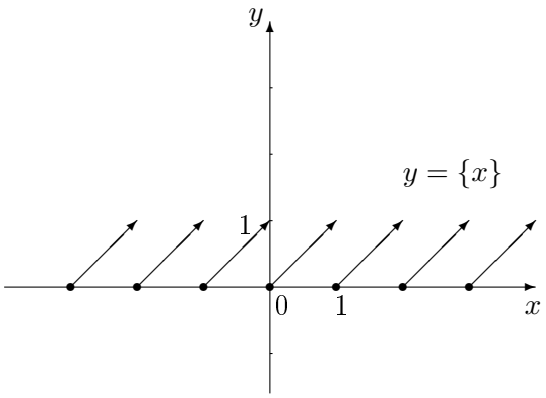
З а д а ч а 3. Найти показатель α, с которым число 3 входит в каноническое разложение 50! на простые множители.

Р е ш е н и е. Применим к условию задачи только что доказанную теорему. Получим: $\alpha = \left[\frac{50}{3}\right] + \left[\frac{50}{9}\right] + \left[\frac{50}{27}\right] + 0 = 16 + 5 + 1 = 22$.

2. Дробная часть действительного числа $\{x\}$.

О п р е д е л е н и е 4. *Дробная часть* действительного числа x определяется как разность числа x и его целой части: $\{x\} \stackrel{\text{df}}{=} x - [x]$.

График функции $y = \{x\}$ имеет вид:



З а д а ч а 4. Вычислить: а) $\{3{,}12\}$; б) $\{0{,}5\}$; в) $\{-1{,}5\}$.

Р е ш е н и е. Используя определение функции $\{x\}$, получим:

а) $\{3{,}12\} = 3{,}12 - 3 = 0{,}12$;

б) $\{0{,}5\} = 0{,}5 - 0 = 0{,}5$;

в) $\{-1{,}5\} = -1{,}5 - (-2) = 0{,}5$.

3. Количество $\tau(n)$ натуральных делителей натурального числа n.

Т е о р е м а 5. *Пусть натуральное число n задано в каноническом виде: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Тогда*

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

Д о к а з а т е л ь с т в о. Мы знаем, что каждый делитель d числа n будет представим в виде канонического разложения $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, причем $0 \leqslant \beta_i \leqslant \alpha_i$ (см. «Предварительные сведения», утверждение 6).

Чтобы найти число натуральных делителей, необходимо подсчитать число всевозможных различных комбинаций для $\beta_1,\ \beta_2,\ \ldots,\ \beta_k$, отвечающих условиям $0 \leqslant \beta_i \leqslant \alpha_i$, так как различным комбинациям значений $\beta_1,\ \beta_2,\ \ldots,\ \beta_k$ соответствуют различные числа d. Поскольку $\beta_1,\ \beta_2,\ \ldots,\ \beta_k$ независимо друг от друга принимают соответственно $\alpha_1 + 1,\ \alpha_2 + 1,\ \ldots,\ \alpha_k + 1$ различных значений, то общее число таких комбинаций будет

$$(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

Таким образом, получаем:

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

Теорема доказана.

З а д а ч а 5. Найти количество натуральных делителей числа 1000000.

Р е ш е н и е. $\tau(1000000) = \tau(2^6 \cdot 5^6) = (6+1)\cdot(6+1) = 49$.

4. Сумма $\sigma(n)$ натуральных делителей натурального числа n.

П р и м е р. Найти сумму натуральных делителей числа 18.

Р е ш е н и е. $\sigma(18) = 1 + 2 + 3 + 6 + 9 + 18 = 39$.

Т е о р е м а 6. *Пусть натуральное число n задано в каноническом виде: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Тогда*

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Д о к а з а т е л ь с т в о. Составим произведение

$$(p_1^0 + p_1^1 + p_1^2 + \ldots + p_1^{\alpha_1}) \cdot (p_2^0 + p_2^1 + p_2^2 + \ldots + p_2^{\alpha_2}) \cdot \ldots \times$$

$$\times (p_k^0 + p_k^1 + p_k^2 + \ldots + p_k^{\alpha_k}).$$

Если раскрыть скобки, то мы получим сумму членов вида: $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, где $0 \leqslant \beta_i \leqslant \alpha_i, \quad i = 1,\ 2,\ \ldots,\ k$. Но все такие члены являются делителями числа n (см. «Предварительные сведения», утверждение 6), причем каждый делитель входит в сумму только один раз. Поэтому произведение указанных выше скобок равно сумме всех натуральных делителей числа n.

Заметим, что каждая сумма в скобках является геометрической прогрессией со знаменателем p_i, $i = 1,\ 2,\ \ldots,\ k$. Применяя формулу суммы геометрической прогрессии, получим:

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Теорема доказана.

З а д а ч а 6. Вычислить $\sigma(18)$.

Р е ш е н и е. $\sigma(18) = \sigma(2 \cdot 3^2) = \dfrac{2^2-1}{2-1} \cdot \dfrac{3^3-1}{3-1} = 3 \cdot 13 = 39$.

Для удобства введем новое обозначение. Символом $\sum\limits_{d|n}$ будем обозначать некоторую сумму, в которой суммирование проведено по всем делителям d числа n, или, другими словами, *сумму, распространенную на все делители натурального числа* n.

Т е о р е м а 7. *Если каноническая запись числа* n *имеет вид* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, *а* $f(n)$ — *мультипликативная функция, то*

$$\sum_{d|n} f(n) = [1 + f(p_1) + f(p_1^2) + \ldots + f(p_1^{\alpha_1})] \times$$
$$\times [1 + f(p_2) + f(p_2^2) + \ldots + f(p_2^{\alpha_2})] \times \ldots \times \qquad (1)$$
$$\times [1 + f(p_k) + f(p_k^2) + \ldots + f(p_k^{\alpha_k})].$$

Д о к а з а т е л ь с т в о. Для доказательства формулы (1) раскроем скобки в правой части равенства и учтем, что по теореме 3

$$f(p_1^{\beta_1}) \cdot f(p_2^{\beta_2}) \cdot \ldots f(p_k^{\beta_k}) = f(p_1^{\beta_1} \cdot {}_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}),$$

причем произведение $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ — есть делитель числа $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Теорема доказана.

Формулы для $\tau(n)$ и $\sigma(n)$, выведенные выше, есть частные случаи общей формулы (1). Чтобы вывести формулу для $\tau(n)$, достаточно положить $f(n) = 1$. Тогда слева получится сумма единиц, причем их число равно числу делителей n, т.е. $\tau(n)$, а справа — произведение чисел

$\alpha_1 + 1,\ \alpha_2 + 1,\ \ldots,\ \alpha_k + 1$. В свою очередь, формула для $\sigma(n)$ получается, если принять $f(n) = n$ (эта функция мультипликативна, проверьте самостоятельно!). Тогда слева получится сумма всех делителей n, а справа — произведение

$$(1 + p_1^1 + p_1^2 + \ldots + p_1^{\alpha_1}) \cdot (1 + p_2^1 + p_2^2 + \ldots + p_2^{\alpha_2}) \cdot \ldots \times$$
$$\times (1 + p_k^1 + p_k^2 + \ldots + p_k^{\alpha_k}).$$

З а м е ч а н и е. С помощью формулы (1) можно получить и новые формулы. Полагая, к примеру, $f(n) = n^\lambda$ (самостоятельно проверьте, что эта функция мультипликативна!), выводим, что при $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

$$\sum_{d|n} n^\lambda = (1+p_1^\lambda+p_1^{2\lambda}+\ldots+p_1^{\lambda\alpha_1})\cdot(1+p_2^\lambda+p_2^{2\lambda}+\ldots+p_2^{\lambda\alpha_2})\cdot\ldots\times$$
$$\times (1 + p_k^\lambda + p_k^{2\lambda} + \ldots + p_k^{\lambda\alpha_k}) =$$
$$= \frac{p_1^{\lambda\alpha_1+1} - 1}{p_1^\lambda - 1} \cdot \frac{p_2^{\lambda\alpha_2+1} - 1}{p_2^\lambda - 1} \cdot \ldots \cdot \frac{p_k^{\lambda\alpha_k+1} - 1}{p_k^\lambda - 1}.$$

5. Функция Мебиуса.

О п р е д е л е н и е 5. *Функцией Мебиуса* $\mu(n)$ называется числовая мультипликативная функция, определенная на степенях простых чисел следующим образом:

$$\mu(p) = -1, \quad \mu(p^k) = 0, \quad k \geqslant 2.$$

Пользуясь свойством мультипликативности функции Мебиуса, ее можно доопределить на всех натуральных числах следующим образом:

1) $\mu(1) = 1$;

2) $\mu(n) = 0$, если n делится на квадрат простого числа, т. е. если в каноническое разложение n входит хотя бы один простой множитель в степени, большей, чем первая;

3) $\mu(p_1p_2\dots p_s) = (-1)^s$, если все простые числа $p_1,\ p_2,\ \dots,\ p_s$ различны.

Примеры.

1. $\mu(90) = \mu(2\cdot 3^2\cdot 5) = 0$;
2. $\mu(77) = \mu(7\cdot 11) = 1$;
3. $\mu(59) = \mu(2^3\cdot 7) = 0$;
4. $\mu(105) = \mu(3\cdot 5\cdot 7) = -1$.

Справедлива теорема:

Теорема 8.

$$\sum_{d|n}\mu(d) = \begin{cases} 1, & \textit{если } n = 1, \\ 0, & \textit{если } n > 1. \end{cases} \qquad (2)$$

Доказательство. Рассмотрим два случая:

1) Пусть $n = 1$. Тогда искомая сумма равна $\mu(1) = 1$ (по определению).

2) Пусть $n > 1$. Тогда существует каноническое разложение $n = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$. Для любого делителя d натурального числа n, содержащего хотя бы одно простое число в степени, большей чем первая, $\mu(d) = 0$; поэтому в сумме (2) можно оставить только делители произведения $p_1p_2\dots p_s$. Количество делителей числа $p_1p_2\dots p_s$, являющихся произведениями k простых чисел из данных, равно, очевидно, количеству всевозможных подмножеств множества $\{p_1,\ p_2,\ \dots,\ p_s\}$, которые состоят из k чисел, т.е. равно числу сочетаний C_s^k. Поэтому, применяя формулу бинома Ньютона, получаем:

$$\sum_{d|n}\mu(d) = \sum_{d|p_1p_2\dots p_s}\mu(d) = \mu(1) + \sum_{\substack{i \\ 1\leqslant i\leqslant s}}\mu(p_i) +$$

$$+ \sum_{\substack{i,\,j \\ 1\leqslant i\leqslant j\leqslant s}} \mu(p_i p_j) + \ldots = 1 - C_s^1 + C_s^2 - \ldots + (-1)^s C_s^s =$$

$$= (1-1)^s = 0,$$

где C_s^k — соответствующие биномиальные коэффициенты. Теорема доказана.

§3. Распределение простых чисел

1. Асимптотический закон распределения простых чисел. Обозначим через $\pi(x)$ функцию, определяющую количество простых чисел на промежутке $[2, x)$ натурального ряда.

На протяжении двух веков (XVIII–XIX) европейские математики К. Ф. Гаусс, А. М. Лежандр и русские математики (П. Л. Чебышев и др.) пытались найти формулу для вычисления этой функции. Результаты этих исследований показали, что распределение простых чисел в натуральном ряду неравномерно и подчиняется весьма сложным закономерностям.

С одной стороны, количество простых чисел бесконечно (теорема Евклида) и в натуральном ряду встречаются пары простых чисел, отличающихся друг от друга на две единицы. Например: 11 и 13, 17 и 19, 41 и 43. Такие пары простых чисел назвали *близнецами*. Вопрос об их конечности или бесконечности не решен до настоящего времени. С другой стороны, в натуральном ряду существуют сколь угодно длинные промежутки, не содержащие простых чисел (теорема об интервалах). Например, в последовательности

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+n$$

при $n \to \infty$ все числа будут составными.

Поскольку из-за сложного характера распределения простых чисел явного выражения для функции $\pi(x)$ найти не удалось, математики попытались получить ее асимптотическое приближение.

О п р е д е л е н и е 7. Две функции $f(x)$ и $\varphi(x)$ называются *асимптотически равными* при $x \to \infty$, если они бесконечно велики при $x \to \infty$ и предел их отношения равен 1, т.е. $\lim\limits_{x\to\infty} \dfrac{f(x)}{\varphi(x)} = 1$. Пишут: $f(x) \sim \varphi(x)$.

Гаусс предположил, что

$$\pi(x) \approx \int\limits_2^x \frac{\mathrm{d}t}{\ln t}.$$

Позднее, в 1808 году французский математик Лежандр опубликовал гипотезу, согласно которой

$$\pi(x) \sim \frac{x}{\ln x - 1,08366}.$$

Эти предположения доказаны не были.

Большой вклад в решение вопроса о распределении простых чисел внес русский математик Пафнутий Львович Чебышев (1821–1894). В 1849 году он доказал, что

$$\pi(x) \sim \frac{x}{\ln x}.$$

Это утверждение получило название *асимптотического закона распределения простых чисел.* Оно равносильно утверждению $\pi(x) \sim \mathrm{li}(x)$, где функция

$$\mathrm{li}(x) = \int\limits_2^x \frac{\mathrm{d}t}{\ln t}$$

называется *интегральным логарифмом* действительного числа x.

Получить окончательное доказательство закона распределения простых чисел П. Л. Чебышеву не удалось — он не доказал существование предела

$$\lim_{x\to\infty}\left(\pi(x) \div \frac{x}{\ln x}\right) = 1,$$

а только строго доказал двойное неравенство

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

(которое получило название — *неравенство Чебышева*) и установил справедливость следующей теоремы:

Т е о р е м а 9. *Для произвольного натурального числа $n > 3$ между числами n и $2n-2$ содержится хотя бы одно простое число.*

Только в конце XIX века (в 1896 году), используя результаты П. Л. Чебышева и Б. Римана, почти одновременно, французский математик Ж. Адамар и бельгийский математик Ш. Валле Пуссен доказали асимптотический закон распределения простых чисел.

2. Простые числа в арифметических прогрессиях. Натуральный ряд чисел является арифметической прогрессией с первым членом 1 и и разностью 1. Поэтому естественно было использовать результаты, полученные при изучении распределения простых чисел в натуральном ряду и при решении вопроса о распределении простых чисел в арифметических прогрессиях. Ограничимся рассмотрением прогрессий, в который первый член a и разность d взаимно просты. В противном случае все члены прогрессии будут делиться на наибольший общий делитель a и d и в прогрессии не будет простых чисел. Случай, когда $(a, d) = 1$,

рассмотрел немецкий математик Л. Дирихле. В 1837 г. он доказал следующее обобщение теоремы Евклида:

Т е о р е м а 10 (Д и р и х л е). *Если* $(a, d) = 1$, *то прогрессия*

$$a,\ a+d,\ \ldots,\ a+(n-1)d,\ \ldots \tag{3}$$

содержит бесконечно много простых чисел.

Еще до этого теорема о бесконечности множества простых чисел в арифметических прогрессиях была доказана для некоторых частных случаев элементарными методами. Докажем для примера следующую теорему:

Т е о р е м а 11. *Множество простых чисел вида* $p = 4n - 1$ *бесконечно.*

Д о к а з а т е л ь с т в о. Из равенства

$$(4m+1)(4n+1) = 16mn + 4m + 4n + 1$$

видно, что произведение двух чисел, каждое из которых при делении на 4 дает в остатке 1, имеет тот же остаток 1 при делении на 4. Отсюда понятно, что ни одно число вида $4n-1$ не может быть разложено в произведение множителей вида $4n+1$.

Предположим, что множество простых чисел вида $4n-1$ конечно и состоит из чисел $p_1,\ p_2,\ \ldots,\ p_k$. Обозначим через N произведение $N = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ и положим $M = 4N - 1$.

Мы выяснили, что M не может раскладываться в произведение простых множителей вида $4m+1$, т.е. имеет хотя бы один простой делитель p вида $4n-1$. Так как по предположению $p_1,\ p_2,\ \ldots,\ p_k$ — простые числа вида $4n-1$, то $M = 4N-1$ должно делиться на одно из этих чисел, например на p_j. Это противоречит тому, что $4N = 4p_1 \cdot p_2 \cdot \ldots \cdot p_k$

делится на p_j, а -1 не делится на p_j. Полученное противоречие указывает на неверность нашего предположения о конечности множества простых чисел вида $4n-1$. Теорема доказана.

Если обозначить через $\pi_a(d,x)$ количество простых чисел в прогрессии (3), не превосходящих x, то теорема Дирихле может быть сформулирована так: если $(d,a)=1$, то $\lim\limits_{x\to+\infty}\pi_a(d,x)=+\infty$. Асимптотический закон для $\pi_a(d,x)$ имеет вид:

$$\pi_a(d,x)\sim\frac{x}{\varphi(d)\ln x},$$

где $\varphi(d)$ — функция Эйлера.

Отметим в заключение, что исследования относительно содержания простых чисел в последовательности натуральных чисел, которая получается, когда в квадратичной функции ax^2+bx+c x пробегает все натуральные значения, даже для частного случая функции x^2+1, до сих пор не имеют успеха.

Глава II. Систематические числа

§1. Системы счисления

1. Непозиционные системы счисления.

О п р е д е л е н и е 1. *Системой счисления* называют язык для наименования, записи чисел и выполнения действий над ними.

Чтобы записать любое натуральное число с помощью определенных индивидуальных знаков, используют различные системы счисления (нумерации), которые можно разбить на две основные группы: *непозиционные* и *позиционные.*

В непозиционных системах счисления значение каждого используемого знака не зависит от его места в записи числа. К таким системам относятся: древнегреческая, славянская, грузинская, армянская, египетская, иероглифическая, римская и другие.

В настоящее время некоторое значение сохранила лишь римская нумерация. В ней используются следующие знаки: I — единица, V — пять, X — десять, L — пятьдесят, C — сто, D — пятьсот, M — тысяча.

Правила записи:

а) если знак, изображающий меньшее число, стоит после знака, изображающего большее число, то производится сложение: $\mathrm{VII} = 5+1+1 = 7,\ \mathrm{CLVI} = 100+50+5+1 = 156.$

б) если знак, изображающий меньшее число, стоит перед знаком, изображающим большее число, то производится вычитание: $\mathrm{IX} = 10 - 1 = 9,\ \mathrm{MCDXXIX} = 1000 + 500 - -100 + 10 + 10 + 10 - 1 = 1429.$

2. Позиционные системы счисления. В позиционных системах счисления значение применяемых знаков (цифр) зависит от места, которое этот символ занимает в записи числа. Например, в десятичной системе счисления используются цифры: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Из них образуются конечные последовательности, которые являются краткими записями чисел.

В записи 3421 знак «3» обозначает три тысячи единиц, а в записи 123 этот же знак обозначает три единицы, т.е. в позиционной системе счисления с основанием g сдвиг цифры на одно место влево влечет за собой увеличение ее значения в (g) раз, где g — любое натуральное число, большее 1.

О п р е д е л е н и е 2. *Систематической записью* натурального числа N по основанию g называют представление этого числа в виде суммы:

$$N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0 = \sum_{i=0}^{n} a_i g^i,$$

где коэффициенты $a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0$ принимают значения $0,\ 1,\ 2,\ \ldots,\ g-1$, причем $a_n \neq 0$.

З а м е ч а н и е. Если основание системы счисления равно g, то число N можно записать короче в виде: $\overline{a_k a_{k-1} \ldots a_1 a_0}_g$.

В настоящее время наибольшее распространение имеют системы счисления по основанию $g = 10$, $g = 16$, $g = 2$. Первая — исторически связана со счетом на пальцах и метрической системой мер, она наиболее удобна при выполнении действий над числами; последние две — с развитием вычислительной математики (ВМ) и информационно-коммуникационных технологий (ИКТ). Дело в том, что для изображения цифр в ЭВМ применяются элементы, способ-

ные находиться в одном из нескольких разграниченных состояний. Число таких состояний должно равняться числу цифр системы счисления, применяемой для ввода информации.

В десятичной системе счисления любое натуральное число будет иметь вид:

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0$$

или $N = \overline{a_n a_{n-1} \ldots a_1 a_0}_{10}$, причем

$$\begin{array}{ccccc} 1 & \leqslant & a_n & \leqslant & 9 \\ 0 & \leqslant & a_{n-1} & \leqslant & 9 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \leqslant & a_0 & \leqslant & 9 \end{array}$$

Место, занимаемое цифрой в записи числа, считая справа налево, называют *разрядом.*

Так,

a_0	— определяет число единиц	1-го	разряда;
a_1	— определяет число единиц	2-го	разряда;
$\ldots$	$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	$\ldots\ldots$	$\ldots\ldots\ldots$
a_n	— определяет число единиц	$(n+1)$-го	разряда.

Каждая единица следующего разряда в 10 раз больше единицы предыдущего разряда, например:

$$456_{10} = 4 \cdot 10^2 + 5 \cdot 10^1 + 6 \cdot 10^0,$$

а в записи

$$231_4 = 2 \cdot 4^2 + 3 \cdot 4^1 + 1 \cdot 4^0$$

каждая единица следующего разряда в 4 раза больше единицы предыдущего разряда, т.е. «3» обозначает 12 единиц, а «2» — 32 единицы.

Т е о р е м а 1. *Любое натуральное число N может быть единственным образом представлено в виде систематической записи по любому основанию $g > 1$.*

Д о к а з а т е л ь с т в о. Пусть g — основание системы счисления, причем $g > 1$. Нужно доказать возможность представления любого натурального числа N в виде:

$$N = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0 \qquad (4)$$

и единственность такого представления, т.е., если

$$(N = \overline{a_k a_{k-1} \ldots a_1 a_0}_g) \ \& \ (N = \overline{b_m b_{m-1} \ldots b_1 b_0}_g),$$

то обязательно $(k = m) \ \& \ (a_i = b_i), \quad i = 0,\ 1,\ 2,\ \ldots,\ k.$

С у щ е с т в о в а н и е. Докажем сначала, что если $0 \leqslant N < g^{k+1}$, то число n допускает запись вида (4). Доказательство проведем методом математической индукции по k.

а) Пусть $k = 0$, тогда $0 \leqslant N < g$ и g-ичная запись числа N будет состоять из одного слагаемого, т.е. $N = a_0$.

б) Пусть для всех $0 \leqslant N < g^k$ существует систематическая запись (4).

в) Докажем существование систематической записи (4) для $g^k \leqslant N < g^{k+1}$. Разделим N на g^k с остатком. Получим $N = a_k g^k + n_1$, где $n_1 < g^k$ и по предложению (б) уже имеет запись вида (4): $n_1 = a_{k-1} g^{k-1} + \ldots + a_1 g + a_0$. Тогда

$$N = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0.$$

Поскольку для любого натурального числа N найдется такое число k, что $N < g^{k+1}$, то возможность g-ичного представления в виде (4) доказана для любого натурального числа.

Единственность. Теперь докажем, что такое представление единственно. Доказательство снова проведем методом математической индукции по k.

а) Если $0 \leqslant N < g$, то $n = a_0$, и систематическая запись числа N будет однозначно определяться одной из цифр 0, 1, 2, $\ldots$, $g-1$.

б) Пусть для всех N, где $0 \leqslant N < g^k$ запись (4) определяется однозначно.

в) Тогда запись для $g^k \leqslant N < g^{k+1}$, где $N = a_k g^k + n_1$, будет тоже определена однозначно, так как частное a_k и остаток n_1 от деления N на g^k определяется однозначно. Теорема доказана.

§2. Переход от одной системы счисления к другой

1. Арифметические операции над систематическими числами. Арифметические операции в любой системе счисления выполняются так же, как и в десятичной системе счисления. Для этого нужно знать таблицы сложения и умножения в данной системе с основанием g.

Например, пусть $g = 4$. Следовательно, в данной системе счисления используются цифры 0, 1, 2, 3. Любое натуральное число n записывается только с помощью этих знаков. Например, $9_{10} = 21_4$. Таблицы сложения и умножения будут иметь вид:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Зная эти таблицы, мы можем сложить, вычесть, умножить и разделить любые два натуральных числа в этой системе счисления. Пусть, к примеру, $a = 121_4$ и $b = 213_4$. Тогда: $a + b = 121_4 + 213_4 = 1000_4$:

$$\begin{array}{r} 121_4 \\ +\ 213_4 \\ \hline 1000_4. \end{array}$$

Проверим этот результат вычитанием:

$$\begin{array}{r} 1\dot{0}\dot{0}0_4 \\ -\ \ 121_4 \\ \hline 213_4. \end{array}$$

$a \cdot b = 121_4 \cdot 213_4 = 33033_4$. Действительно,

$$\begin{array}{r} \times\ 121_4 \\ \ \ 213_4 \\ \hline \ \ 1023 \\ +\ \ 121 \\ \ \ 302 \\ \hline 33033_4. \end{array}$$

Проверим результат делением:

$$\begin{array}{r|l} -\ 33033_4 & 121_4 \\ \cline{2-2} \ \ 302 & 213_4 \\ \cline{1-1} -\ \ 223 & \\ \ \ 121 & \\ \cline{1-1} -\ \ 1023 & \\ \ \ 1023 & \\ \cline{1-1} \ \ 0. & \end{array}$$

2. Перевод чисел из одной системы счисления в другую. Однако, на практике может случиться так, что числа a и b заданы в разных системах счисления. Поэтому возникает задача о переводе записи числа N из одной системы счисления в другую. К решению этой задачи существует два подхода:

а) Перевести оба числа в десятичную систему счисления и в ней выполнить указанные действия, а затем результат записать в требуемой (g-ичной) системе счисления;

б) Научиться переходить от одной системы счисления с основанием g к другой системе — с основанием h и наоборот.

Рассмотрим оба подхода.

а) Пусть

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

$$b = \overline{b_m b_{m-1} \dots b_1 b_0}_g = b_m g^m + b_{m-1} g^{m-1} + \dots + b_1 g + b_0.$$

Чтобы найти десятичные записи этих чисел, достаточно выполнить указанные действия. Рассмотрим теперь способ, позволяющий переводить числа из десятичной системы счисления в произвольную g-ичную систему счисления.

Пусть g-ичная запись числа N имеет вид:

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

Тогда

$$N = n_1 \cdot h + b_0,$$

где

$$n_1 = a_n g^{n-1} + a_{n-1} g^{n-2} + \dots + a_1. \qquad (5)$$

Так как $0 \leqslant a_0 < g$, то a_0 — остаток от деления N на g, а n_1 — частное от этого деления. Из равенства (5) видно, что a_1 — остаток от деления n_1 на g и т.д.

Таким образом, g-ичная запись числа N находится следующим образом. Число N делим (в десятичной системе счисления) на g. Остаток от деления даст последнюю цифру g-ичной записи N. Частное n_1 снова делим на g и новый остаток даст предпоследнюю цифру g-ичной записи N. Продолжая этот процесс деления, найдем все цифры g-ичной записи.

З а д а ч а 1. Найти сумму чисел $a = 341_5$ и $b = 126_7$.

Р е ш е н и е. Переведем оба числа в десятичную систему счисления:

$$a = 3 \cdot 5^2 + 4 \cdot 5 + 1 = 3 \cdot 25 + 20 + 1 = 96_{10};$$

$$b = 1 \cdot 7^2 + 2 \cdot 7 + 6 = 49 + 14 + 6 = 69_{10}.$$

Тогда

$$a + b = 96_{10} + 69_{10} = 165_{10}.$$

Этот результат можно записать в пятеричной и семеричной системах счисления.

Пятеричная запись числа 165 будет иметь вид:

$$165 = a_n \cdot 5^n + a_{n-1} \cdot 5^{n-1} + \ldots + a_1 \cdot 5 + a_0$$

или

$$165 = \underbrace{(a_n \cdot 5^{n-1} + a_{n-1} \cdot 5^{n-2} + \ldots + a_1)}_{n_1} \cdot 5 + a_0,$$

т.е.

$$165 = n_1 \cdot 5 + a_0.$$

Мы видим, что последняя цифра в пятеричной записи числа 165 есть остаток от деления этого числа на основание системы счисления $g = 5$. Предпоследняя цифра a_1 будет остатком от деления n_1 на 5, и т.д.

Найдем пятеричную запись числа 165:

$$\begin{array}{r|l} 165 & 5 \\ \hline 15 & 33 \\ \hline 15 & 30 \\ \hline \textcircled{0} = a_0 & \textcircled{3} = a_1 \end{array} \qquad \begin{array}{r|l} 5 & \\ \hline 6 & 5 \\ \hline 5 & \textcircled{1} = a_2 \end{array} \qquad \begin{array}{r|l} 5 & \\ \hline \textcircled{1} = a_3 & \end{array}$$

Полученные остатки записываем в обратной последовательности в пятеричной системе: $165_{10} = 1130_5$. Проверка: $1130_5 = 1 \cdot 5^3 + 1 \cdot 5^2 + 3 \cdot 5 + 0 = 125 + 25 + 15 = 165_{10}$. Самостоятельно запишите число 165 в семеричной системе счисления.

б) Теперь выясним, как перейти от g-ичной системы счисления к h-ичной. Пусть

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

Нужно записать это число в h-ичной системе, т.е. представить его в виде

$$N = b_m h^m + b_{m-1} h^{m-1} + \ldots + b_1 h + b_0.$$

Тогда

$$N = \underbrace{(b_m h^{m-1} + b_{m-1} h^{m-2} + \ldots + b_1)}_{n_1} \cdot h + b_0$$

или

$$N = n_1 \cdot h + b_0,$$

где b_0 — остаток от деления N на k в g-ичной системе. Понятно, что b_1 будет остатком от деления n_1 на h и т.д. Так как неполные частные убывают, то процесс деления закончится, когда на некотором шаге n_i станет меньше h. Таким образом, цифры в искомой записи числа

$N = \overline{b_m b_{m-1} \dots b_1 b_{0h}}$ есть остатки от деления N на h, n_1 на h, $\dots$, n_i на h, записанные в обратном порядке.

Однако, если $h > g$, то в g-ичной системе счисления некоторые остатки, возможно, будут содержать больше одной цифры; их следует записать новыми, не содержащимися в g-ичной системе счисления h-ичными цифрами.

З а м е ч а н и е. В процессе решения задачи 1 нам потребовалось перевести число из десятичной системы счисления в пятеричную и семеричную системы. В пункте б) возможность подобного перевода чисел из системы счисления с одним основанием в систему счисления с другим основанием обоснована в общем виде. Поэтому первый подход есть частный случай второго.

З а д а ч а 2. Записать число 32014_5 в восьмеричной системе счисления.

Р е ш е н и е. Новое основание системы счисления h равно 8. Так как в пятеричной системе счисления $8 = 13_5$, то делим 32014_5 на 13_5. Получим:

$$
\begin{array}{l|l}
32014_5 & 13_5 \\
\cline{2-2}
31 & 2031_5 \\
\cline{1-1}
101 & 13 \\
\cline{1-1}
44 & 23 \\
\cline{1-1}
24 & 13 \\
\cline{1-1}
13 & 101 \\
\cline{1-1}
11_5 & 44 \\
\cline{2-2}
 & 2_5
\end{array}
\qquad
\begin{array}{l|l}
13_5 & \\
\cline{2-2}
113_5 & 13_5 \\
\cline{2-2}
112 & 4_5 \\
\cline{1-1}
1_5 &
\end{array}
$$

Возвращаясь к восьмеричной системе счисления, выпишем все получившиеся в процессе деления остатки в обратном порядке. Итак, $32014_5 = 4126_8$.

Глава III. Цепные дроби

§1. Конечные цепные дроби

1. Представление рациональных чисел конечными цепными дробями. Рациональные числа можно задавать в разной форме, например, одно и то же число можно записать в виде отношения двух целых чисел $\frac{a}{b}$ или в виде десятичной дроби, причем эта дробь может быть конечной или бесконечной. Запись в виде десятичной дроби имеет ряд существенных преимуществ особенно при приближенных вычислениях, расчетах и т.д.

Здесь мы рассмотрим другую форму записи рациональных чисел, а именно представление их в виде так называемых непрерывных или цепных дробей. Большим преимуществом аппарата цепных дробей является то, что выражение любого рационального числа в виде цепной дроби не зависит от каких-либо других величин, кроме самого этого числа.

Пусть дано рациональное число $\frac{a}{b}$, причем $b > 0$. Применяя к a и b алгоритм Евклида для определения их наибольшего общего делителя (см. «Алгебра», часть 1), получаем конечную систему равенств:

$$\begin{cases} a = bq_0 + r_1 \\ b = r_1q_1 + r_2 \\ r_1 = r_2q_2 + r_3 \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n \\ r_{n-1} = r_nq_n + 0. \end{cases} \tag{6}$$

Системе равенств (6) соответствует равносильная систе-

ма

$$\begin{cases} \dfrac{a}{b} = q_0 + \dfrac{r_1}{b} = q_0 + \dfrac{1}{\frac{b}{r_1}} \\ \dfrac{b}{r_1} = q_1 + \dfrac{r_2}{r_1} = q_1 + \dfrac{1}{\frac{r_1}{r_2}} \\ \dfrac{r_1}{r_2} = q_2 + \dfrac{r_3}{r_2} = q_2 + \dfrac{1}{\frac{r_2}{r_3}} \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ \dfrac{r_{n-2}}{r_{n-1}} = q_{n-1} + \dfrac{r_n}{r_{n-1}} = q_{n-1} + \dfrac{1}{\frac{r_{n-1}}{r_n}} \\ \dfrac{r_{n-1}}{r_n} = q_n, \end{cases} \qquad (6')$$

из которой последовательной заменой каждой из дробей $\dfrac{b}{r_1}$, $\dfrac{r_1}{r_2}$ и т.д. ее соответствующим выражением из следующей строки получается представление дроби $\dfrac{a}{b}$ в виде:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}}. \qquad (7)$$

Заметим, что ввиду последнего из равенств $(6')$ $q_n > 1$

при $(n > 0)$. Сокращенно дробь вида (7) будем обозначать:

$$\frac{a}{b} = [q_0;\ q_1,\ q_2,\ \ldots,\ q_n].$$

О п р е д е л е н и е 1. Представление (7) рационального числа $\frac{a}{b}$ называется *конечной цепной* или *непрерывной дробью.*

Числа $q_0,\ q_1,\ q_2,\ \ldots,\ q_n$ называются неполными частными числа $\frac{a}{b}$, причем $q_0 \in \mathbb{Z}$, а $q_1,\ q_2,\ \ldots,\ q_n \in \mathbb{N}$.

Имеет место *теорема существования и единственности разложения всякого рационального числа в конечную цепную дробь.*

Т е о р е м а 1. *Всякое рациональное число может быть представлено в виде конечной цепной дроби единственным образом, если* $q_n > 1$.

Д о к а з а т е л ь с т в о.

С у щ е с т в о в а н и е. Выше мы представили алгоритм, позволяющий любое рациональное число $\frac{a}{b}$ разложить в конечную цепную дробь, т.е. доказали существование такого разложения.

Е д и н с т в е н н о с т ь. Теперь докажем (от противного), что представление любого рационального числа в виде конечной цепной дроби при условии $q_n > 1$, единственно.

Пусть возможны два представления числа $\frac{a}{b}$ в виде конечной цепной дроби:

$$\frac{a}{b} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_n]; \quad \frac{a}{b} = [b_0;\ b_1,\ b_2,\ \ldots,\ b_k]. \qquad (8)$$

Тогда

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}}} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \ddots + \cfrac{1}{b_k}}}}.$$

Рассмотрим второе слагаемое левой части равенства, обозначив его через c:

$$c = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}}}.$$

Здесь все a_i — натуральные числа.

Если $n > 1$, то $0 < c < 1$.

Если $n = 1,\ a_1 > 1$, то и в этом случае $0 < c < 1$.

Если $n = 1$ и $a_n = 1$, то $c = 1$. Поскольку этот случай исключается (по условию теоремы), то $0 < c < 1$ всегда, т.е. c — правильная дробь.

Тогда:

$$\frac{a}{b} = a_0 + c, \text{ где } 0 < c < 1.$$

Аналогично:

$$\frac{a}{b} = b_0 + l, \text{ где } 0 < l < 1.$$

Это значит, что a_0 и b_0 — целые части одного и того же числа $\dfrac{a}{b}$. Но так как целая часть числа определяется однозначно, то $a_0 = b_0$.

После вычитания a_0 и b_0 из обеих частей равенства (8) получим равные дроби с равными числителями, но тогда и знаменатели этих дробей равны, т.е.

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}} = b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \ddots + \cfrac{1}{b_k}}}.$$

Рассуждая совершенно аналогично, получим последовательно: $a_1 = b_1,\ a_2 = b_2,\ \ldots$, и т.д.

Далее возможны три случая:

1) $n = k$; 2) $n < k$; 3) $n > k$.

Первый случай. $n = k$. Тогда получим:

$$a_0 = b_0,\ a_1 = b_1,\ \ldots,\ a_n = b_k.$$

Теорема доказана.

Второй случай. $n < k$. Имеем:

$$a_n = b_n + \cfrac{1}{b_{n+1} + \ddots + \cfrac{1}{b_k}},$$

причем a_n — целое число. Правая часть этого равенства может быть целым числом лишь при $k = n + 1$ и $b_{n+1} = 1$, но это противоречит условию $b_k > 1$. Значит, случай $n < k$ невозможен.

Точно так же доказывается невозможность третьего случая (когда $n > k$). Остается только первый случай:

$$n = k;\ a_0 = b_0,\ a_1 = b_1,\ \ldots,\ a_n = b_k.$$

Теорема полностью доказана.

З а м е ч а н и е. Если не требовать, чтобы последний элемент q_n $(n > 0)$ цепной дроби был больше 1, то любое рациональное число наряду с (7) будет представимо в виде

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{(q_n - 1) + \cfrac{1}{1}}}}.$$

З а д а ч а 1. Разложить рациональные числа в цепные дроби:

а) $\frac{35}{26}$; б) $\frac{1}{17}$; в) 9; г) -12.

Р е ш е н и е.

а) Применим к числам $a = 35$ и $b = 26$ алгоритм Евклида:

$$\begin{array}{r|l} 35 & 26 \\ \hline 26 & 1 \end{array} \qquad \begin{array}{r|l} 26 & 9 \\ \hline 18 & 2 \end{array} \qquad \begin{array}{r|l} 9 & 8 \\ \hline 8 & 1 \end{array} \qquad \begin{array}{r|l} 8 & 1 \\ \hline 8 & 8 \end{array} \qquad 0$$

или

$$\begin{aligned} 35 &= 26 \cdot 1 + 9 \\ 26 &= 9 \cdot 2 + 8 \\ 9 &= 8 \cdot 1 + 1 \\ 8 &= 1 \cdot 8 + 0. \end{aligned}$$

Таким образом, $\dfrac{35}{26} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{8}}} = [1;\ 2,\ 1,\ 8]$.

б) Здесь очевидно, что $\dfrac{1}{17} = 0 + \dfrac{1}{17} = [0;\ 17]$.

в) Понятно, что $9 = [9]$.

г) Аналогично, $-12 = [-12]$.

Т е о р е м а 2. *Всякая конечная цепная дробь есть рациональное число.*

Д о к а з а т е л ь с т в о. Для доказательства достаточно выполнить указанные арифметические действия над целыми числами 1 и q_i в разложении дроби (7). Тогда получим снова дробь, т.е. рациональное число. Теорема доказана.

З а д а ч а 2. Для цепной дроби $\dfrac{a}{b} = [2;\ 2,\ 7]$ найти числитель a и знаменатель b.

Р е ш е н и е. $\dfrac{a}{b} = 2 + \cfrac{1}{2 + \cfrac{1}{7}} = 2 + \dfrac{7}{14 + 1} = 2 + \dfrac{7}{15} = \dfrac{37}{15}$.

Итак, $a = 37$, $b = 15$.

З а м е ч а н и е. Из теорем 1 и 2 следует, что рациональные числа и только они могут быть представлены конечными цепными дробями.

2. Подходящие дроби и их свойства. Пусть дано некоторое рациональное число, разложенное в цепную дробь:

$$\frac{a}{b} = [q_0;\ q_1,\ q_2,\ \ldots,\ q_n]. \tag{8}$$

Образуем из нее цепные дроби:

$[q_0]$; $[q_0;\ q_1]$; $[q_0;\ q_1,\ q_2]$; $\ldots$; $[q_0;\ q_1,\ q_2,\ \ldots,\ q_n] = \dfrac{a}{b}$.

Каждая из таких дробей называется отрезком цепной дроби (8) или *подходящей дробью*. Подходящие дроби можно представить в виде:

$$[q_0] = q_0 = \frac{P_0}{Q_0},\ \text{где } P_0 = q_0,\ Q_0 = 1;$$

$$[q_0;\ q_1] = q_0 + \frac{1}{q_1} = \frac{q_0 q_1 + 1}{q_1} = \frac{P_1}{Q_1},$$
$$\text{где } P_1 = q_0 q_1 + 1,\ Q_1 = q_1;$$

$$[q_0;\ q_1,\ q_2] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}} = q_0 + \frac{q_2}{q_1 q_2 + 1} =$$
$$= \frac{(q_1 q_2 + 1)q_0 + q_2}{q_1 q_2 + 1} = \frac{P_2}{Q_2},$$
$$\text{где } P_2 = (q_1 q_2 + 1)q_0 + q_2,\ Q_2 = q_1 q_2 + 1;\ \text{и т.д.}$$

О п р е д е л е н и е 2. *Последовательность*

$$\frac{P_0}{Q_0};\ \frac{P_1}{Q_1};\ \frac{P_2}{Q_2};\ \ldots;\ \frac{P_n}{Q_n}$$

называется последовательностью подходящих дробей k-ого порядка, где $k = 0,\ 1,\ 2,\ \ldots,\ n$.

Ясно, что последняя подходящая дробь $\dfrac{P_n}{Q_n}$ есть число $\dfrac{a}{b}$.

З а д а ч а 3. Дано разложение числа $\dfrac{175}{52}$ в виде цепной дроби: $\dfrac{175}{52} = [3;\ 2,\ 1,\ 2,\ 1,\ 4]$. Найти подходящие дроби нулевого, первого и второго порядков.

Р е ш е н и е. $\dfrac{P_0}{Q_0} = [3] = 3; \quad \dfrac{P_1}{Q_1} = [3;\ 2] = 3 + \dfrac{1}{2} = \dfrac{7}{2};$

$$\frac{P_2}{Q_2} = [3;\ 2,\ 1] = 3 + \cfrac{1}{2 + \cfrac{1}{1}} = 3 + \frac{1}{3} = \frac{10}{3}.$$

Найдем общую формулу для вычисления числителей и знаменателей подходящих дробей произвольного k-ого порядка, где $k = 0,\ 1,\ 2,\ \ldots,\ n$. Справедлива теорема:

Т е о р е м а 3. Числители и знаменатели подходящих дробей вычисляются по рекуррентным формулам:

$$P_k = P_{k-1}q_k + P_{k-2}; \qquad Q_k = Q_{k-1}q_k + Q_{k-2}. \tag{9}$$

Д о к а з а т е л ь с т в о. Проведем доказательство методом математической индукции по порядку k.

1. Проверим, что формулы (9) имеют место при $k = 2$. Здесь мы выбрали в качестве базы индукции номер $k = 2$, так как при $k = 0$ и $k = 1$ рекуррентные формулы теряют смысл; к тому же числа $P_0,\ Q_0,\ P_1,\ Q_1$ нами уже определены (см. выше). Имеем:

$$\frac{P_2}{Q_2} = \frac{(q_1q_2 + 1)q_0 + q_2}{q_1q_2 + 1} = \frac{(q_0q_1 + 1)q_2 + q_0}{q_1q_2 + 1} = \frac{P_1q_2 + P_0}{Q_1q_2 + Q_0}.$$

2. Предположим, что для подходящей дроби k-ого порядка справедлива формула (индуктивное предположение):

$$\frac{P_k}{Q_k} = \frac{P_{k-1}q_k + P_{k-2}}{Q_{k-1}q_k + Q_{k-2}}.$$

3. Докажем теперь, что

$$\frac{P_{k+1}}{Q_{k+1}} = \frac{P_kq_{k+1} + P_{k-1}}{Q_kq_{k+1} + Q_{k-1}}.$$

По определению подходящей дроби $(k+1)$-ого порядка будем иметь:

$$\frac{P_{k+1}}{Q_{k+1}} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k + \cfrac{1}{q_{k+1}}}}}}}.$$

Заметив, что подходящая дробь $(k+1)$-ого порядка получается путем замены q_k на $q_k + \dfrac{1}{q_{k+1}}$, и подставив в числитель и знаменатель формулы индуктивного предположения $q_k + \dfrac{1}{q_{k+1}}$ вместо q_k, получим:

$$P_{k+1} = P_{k-1}\left(q_k + \frac{1}{q_{k+1}}\right) + P_{k-2} =$$

$$= \frac{P_{k-1}(q_k q_{k+1} + 1) + P_{k-2}q_{k+1}}{q_{k+1}} =$$

$$= \frac{q_{k+1}(P_{k-1}q_k + P_{k-2}) + P_{k-1}}{q_{k+1}} = \frac{P_k q_{k+1} + P_{k-1}}{q_{k+1}}.$$

Аналогично,

$$Q_{k+1} = Q_{k-1}\left(q_k + \frac{1}{q_{k+1}}\right) + Q_{k-2} =$$

$$= \frac{Q_{k-1}(q_k q_{k+1} + 1) + Q_{k-2}q_{k+1}}{q_{k+1}} =$$

$$= \frac{q_{k+1}(Q_{k-1}q_k + Q_{k-2}) + Q_{k-1}}{q_{k+1}} = \frac{Q_k q_{k+1} + Q_{k-1}}{q_{k+1}},$$

тогда

$$\frac{P_{k+1}}{Q_{k+1}} = \frac{P_k q_{k+1} + P_{k-1}}{Q_k q_{k+1} + Q_{k-1}}.$$

Следовательно, на основании принципа математической индукции, заключаем, что для любого натурального числа k формулы (9) имеют место. Теорема доказана.

Выпишем рекуррентные формулы для вычисления числителей P_k и знаменателей Q_k подходящих дробей *(закон составления подходящих дробей)*:

$P_0 = q_0, \quad P_1 = q_0 q_1 + 1,$ а при $k \geqslant 2 \quad P_k = P_{k-1}q_k + P_{k-2};$

$Q_0 = 1, \quad Q_1 = q_1, \qquad\qquad Q_k = Q_{k-1}q_k + Q_{k-2}.$

З а м е ч а н и е. Вычисление подходящих дробей k-тых порядков по формулам (9) наиболее удобно проводить по следующей схеме:

k		0	1	2	...
q_k		q_0	q_1	q_2	...
P_k	1	$P_0 = q_0$	$P_1 = q_0 q_1 + 1$	$P_2 = P_1 q_2 + P_0$	...
Q_k	0	$Q_0 = 1$	$Q_1 = q_1$	$Q_2 = Q_1 q_2 + Q_0$	...

k	...	k	k+1	...	n
q_k	...	q_k	q_{k+1}	...	q_n
P_k	...	$P_k = P_{k-1}q_k + P_{k-2}$	...	...	P_n
Q_k	...	$Q_k = Q_{k-1}q_k + Q_{k-2}$	...	...	Q_n

(продолжение)

Например, для нахождения P_{k+1} надо стоящее над ним число q_{k+1} умножить на стоящее слева от клетки для P_{k+1}

число P_k и к результату прибавить стоящее слева от P_k число P_{k-1}. Аналогичным способом вычисляется и Q_{k+1}.

Правильность сделанных вычислений проверяется совпадением последних вычисленных выражений для P_n и Q_n с числителем a и знаменателем b дроби $\dfrac{a}{b}$ соответственно (если $\dfrac{a}{b}$ несократима).

З а д а ч а 4. Дано разложение некоторого рационального числа: $\dfrac{a}{b} = [2;\ 1,\ 1,\ 3,\ 1,\ 2,\ 1,\ 1,\ 2,\ 2]$. Найти это число.

Р е ш е н и е. Имеем: $\dfrac{a}{b} = \dfrac{P_n}{Q_n}$. Для решения задачи нужно вычислить все подходящие дроби, последняя из которых и будет равна $\dfrac{a}{b}$. Составим таблицу:

k		0	1	2	3	4	5	6	7	8	9
q_k		2	1	1	3	1	2	1	1	2	2
P_k	1	2	3	5	18	23	64	87	151	389	929
Q_k	0	1	1	2	7	9	25	34	59	152	363

Таким образом, $\dfrac{P_9}{Q_9} = \dfrac{929}{363} \to \dfrac{a}{b} = \dfrac{929}{363}$.

Т е о р е м а 4. *Знаменатели подходящих дробей — натуральные числа и образуют возрастающую последовательность.*

Д о к а з а т е л ь с т в о. Действительно, $Q_0 = 1$, $Q_1 = q_1 \geqslant 1$, т.к. $q_1 \in \mathbb{N}$, а при $k \geqslant 2$ $Q_k = Q_{k-1}q_k + Q_{k-2}$, где $q_k \geqslant 1$, $Q_{k-1} \geqslant 1$, $Q_{k-2} \geqslant 1$. Поэтому $Q_k > Q_{k-1}$.

Т е о р е м а 5. *Числители и знаменатели двух сосед-*

них подходящих дробей связаны соотношением:

$$P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k. \tag{10}$$

Доказательство. Докажем эту формулу методом математической индукции.

1. Пусть $k = 1$, тогда:

$$P_0 = q_0, \quad Q_0 = 1;$$

$$P_1 = q_0q_1 + 1, \quad Q_1 = q_1$$

и $P_0Q_1 - P_1Q_0 = q_0q_1 - (q_0q_1 + 1) = -1 = (-1)^1$.

2. Предположим, что формула (10) имеет место для подходящих дробей $\dfrac{P_{k-1}}{Q_{k-1}}$ и $\dfrac{P_k}{Q_k}$, т.е. $P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k$.

3. Докажем, что соотношение (10) справедливо для подходящих дробей $\dfrac{P_k}{Q_k}$ и $\dfrac{P_{k+1}}{Q_{k+1}}$. Действительно,

$$P_kQ_{k+1} - P_{k+1}Q_k = P_k(Q_kq_{k+1} + Q_{k-1}) - (P_kq_{k+1} + P_{k-1})Q_k =$$

$$= P_kQ_kq_{k+1} + P_kQ_{k-1} - Q_kP_kq_{k+1} - Q_kP_{k-1} =$$

$$= -(P_{k-1}Q_k - P_kQ_{k-1}) = -(-1)^k = (-1)^{k+1}.$$

Итак, для любого натурального числа n формула (10) верна.

Теорема 6. *Любая подходящая дробь несократима.*

Доказательство. Пусть дана подходящая дробь k-ого порядка $\dfrac{P_k}{Q_k}$. Нужно доказать, что $(P_k,\ Q_k) = 1$. По теореме (5) будем иметь: $P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k$. Если допустить, что $(P_k,\ Q_k) = d > 1$, то левая часть этого

равенства будет делиться на d, а следовательно, и правая часть должна будет делиться на d, но $(-1)^k$ не делится на $d > 1$. Поэтому $(P_k,\ Q_k) = 1$. Теорема доказана.

З а м е ч а н и е. Если рациональное число $\dfrac{a}{b}$ разложить в цепную дробь, то последняя подходящая дробь $\dfrac{P_n}{Q_n}$ в этом разложении несократима и равна $\dfrac{a}{b}$, т.е. разложение в цепную дробь позволяет сокращать дроби.

З а д а ч а 5. Сократить дробь $\dfrac{2329}{9911}$.

Р е ш е н и е. Разложим данное число в цепную дробь. Будем иметь

$$\frac{2329}{9911} = [0;\ 4,\ 3,\ 1,\ 10,\ 1,\ 2].$$

Находим дробь $\dfrac{P_n}{Q_n}$, последовательно заполняя таблицу:

k		0	1	2	3	4	5	6
q_k		0	4	3	1	10	1	2
P_k	1	0	1	3	4	43	47	137
Q_k	0	1	4	13	17	183	200	583

Получаем: $\dfrac{2329}{9911} = \dfrac{P_6}{Q_6} = \dfrac{137}{583}$, причем дробь $\dfrac{137}{583}$ несократима по теореме 6.

Т е о р е м а 7. *Подходящие дроби четного порядка образуют возрастающую, а нечетного — убывающую последовательность.*

Доказательство. Используя формулы (9) и (10), получим:

$$\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} = \frac{P_{k-2}Q_k - P_kQ_{k-2}}{Q_{k-2}Q_k} =$$

$$= \frac{P_{k-2}(Q_{k-1}q_k + Q_{k-2}) - (P_{k-1}q_k + P_{k-2})Q_{k-2}}{Q_{k-2}Q_k} =$$

$$= \frac{P_{k-2}Q_{k-1}q_k + P_{k-2}Q_{k-2} - P_{k-1}Q_{k-2}q_k - P_{k-2}Q_{k-2}}{Q_{k-2}Q_k} =$$

$$= \frac{q_k(P_{k-2}Q_{k-1} - P_{k-1}Q_{k-2})}{Q_{k-2}Q_k} = \frac{q_k(-1)^{k-1}}{Q_{k-2}Q_k}.$$

Итак,

$$\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} = \frac{q_k(-1)^{k-1}}{Q_{k-2}Q_k}.$$

Возможны два случая:

а) Если k — четное, то $\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} < 0$ или $\frac{P_{k-2}}{Q_{k-2}} < \frac{P_k}{Q_k}$, следовательно подходящие дроби четного порядка образуют возрастающую последовательность.

б) Если k — нечетное, то $\frac{P_{k-2}}{Q_{k-2}} - \frac{P_k}{Q_k} > 0$ или $\frac{P_{k-2}}{Q_{k-2}} > \frac{P_k}{Q_k}$, т.е. подходящие дроби нечетного порядка образуют убывающую последовательность. Теорема доказана.

Замечание. Из доказанной теоремы следует, что $\frac{P_0}{Q_0}$ — наименьшая подходящая дробь, а $\frac{P_1}{Q_1}$ — наибольшая подходящая дробь.

Теорема 8. *Любая подходящая дробь* $\frac{P_k}{Q_k}$ *четного порядка меньше подходящих дробей* $\frac{P_{k-1}}{Q_{k-1}}$ *и* $\frac{P_{k+1}}{Q_{k+1}}$.

Доказательство. Дроби $\frac{P_{k-1}}{Q_{k-1}}$ и $\frac{P_{k+1}}{Q_{k+1}}$ — соседние с дробью $\frac{P_k}{Q_k}$, поэтому используя формулу (10), получим:

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_kQ_{k-1} - P_{k-1}Q_k}{Q_kQ_{k-1}} =$$

$$= \frac{-\left(P_kQ_{k-1} - P_{k-1}Q_k\right)}{Q_kQ_{k-1}} = \frac{-\left(-1\right)^k}{Q_kQ_{k-1}} = \frac{(-1)^{k+1}}{Q_kQ_{k-1}}.$$

Аналогично, заменяя k на $k+1$, заключаем, что

$$\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} = \frac{(-1)^{k+2}}{Q_kQ_{k+1}}.$$

Если k — четно, то $(-1)^{k+1} = -1 < 0$, $(-1)^{k+2} > 0$. Следовательно, при четном k

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} < 0, \text{ или } \frac{P_k}{Q_k} < \frac{P_{k-1}}{Q_{k-1}} \quad \text{и}$$

$$\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} > 0, \text{ или } \frac{P_k}{Q_k} < \frac{P_{k+1}}{Q_{k+1}}.$$

Теорема доказана.

Следствие. *Каждая подходящая дробь* $\frac{P_k}{Q_k}$ *нечетного порядка больше подходящих дробей* $\frac{P_{k-1}}{Q_{k-1}}$ *и* $\frac{P_{k+1}}{Q_{k+1}}$.

Доказательство. Положив в доказательстве теоремы (8) порядок подходящей дроби k нечетным, легко приходим к неравенствам:

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} > 0, \text{ или } \frac{P_k}{Q_k} > \frac{P_{k-1}}{Q_{k-1}}, \quad \text{а также}$$

$$\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k} < 0, \text{ или } \frac{P_k}{Q_k} > \frac{P_{k+1}}{Q_{k+1}}$$

(проверьте это самостоятельно!). Следствие доказано.

Т е о р е м а 9. *Любая подходящая дробь четного порядка меньше любой подходящей дроби нечетного порядка.*

Д о к а з а т е л ь с т в о. В силу теоремы (7) и следствия к теореме (8) при $r \geqslant s$ будем иметь:

$$\frac{P_{2r+2}}{Q_{2r+2}} < \frac{P_{2r+1}}{Q_{2r+1}} \leqslant \frac{P_{2s+1}}{Q_{2s+1}}.$$

При $r < s$ получаем:

$$\frac{P_{2r+2}}{Q_{2r+2}} < \frac{P_{2s+2}}{Q_{2s+2}} < \frac{P_{2s+1}}{Q_{2s+1}}.$$

Следовательно, при любых соотношениях между r и s будет справедливо неравенство

$$\frac{P_{2r+2}}{Q_{2r+2}} < \frac{P_{2s+1}}{Q_{2s+1}}.$$

Теорема доказана.

Т е о р е м а 10. *При разложении рационального числа $\frac{a}{b}$ в цепную дробь четные подходящие дроби дают приближение по недостатку, а нечетные — по избытку (за исключением последней дроби, совпадающей с $\frac{a}{b}$).*

Д о к а з а т е л ь с т в о. Если последняя подходящая дробь, совпадающая с числом $\frac{a}{b}$, четного порядка, то она (по теореме (7)) больше всех остальных подходящих дробей четного порядка, которые дают, таким образом, приближения $\frac{a}{b}$ по недостатку. Но при том число $\frac{a}{b}$ как подходящая

дробь четного порядка меньше любой подходящей дроби нечетного порядка (по теореме (8)), а потому подходящие дроби нечетного порядка дают для $\frac{a}{b}$ приближение с избытком. Совершенно аналогично можно рассмотреть случай, когда последняя подходящая дробь, совпадающая с $\frac{a}{b}$, является дробью нечетного порядка. Теорема доказана.

Рассмотренные выше свойства подходящих дробей позволяют сделать следующие выводы:

а) при разложении рационального числа $\frac{a}{b}$ в цепную дробь $[q_0;\ q_1, q_2,\ \ldots,\ q_n]$ образуются две встречных последовательности подходящих дробей:

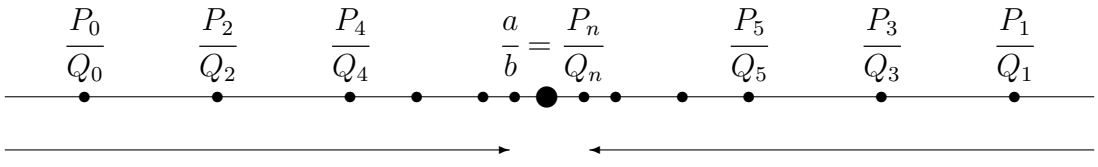
$$\frac{P_0}{Q_0};\ \frac{P_2}{Q_2};\ \frac{P_4}{Q_4};\ \ldots;\ \frac{P_{2k}}{Q_{2k}}$$

— возрастающая последовательность подходящих дробей четного порядка, и

$$\frac{P_1}{Q_1};\ \frac{P_3}{Q_3};\ \frac{P_5}{Q_5};\ \ldots;\ \frac{P_{2k+1}}{Q_{2k+1}}$$

— убывающая последовательность подходящих дробей нечетного порядка.

б) Подходящие дроби четного порядка приближаются к числу $\frac{a}{b}$ по недостатку, а нечетного порядка — по избытку (за исключением последней подходящей дроби $\frac{P_n}{Q_n} = \frac{a}{b}$):



§2. Бесконечные цепные дроби

1. Сходимость бесконечных цепных дробей. Ранее мы установили, что рациональные числа могут изображаться с помощью конечных цепных дробей и, наоборот, свертывание такой конечной непрерывной дроби приводит к рациональной дроби. Оказывается, с помощью бесконечных выражений, аналогичных рассмотренным в §1 этой главы, могут быть изображены всевозможные иррациональные числа.

О п р е д е л е н и е 3. Выражение вида

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n + \ddots}}}}, \tag{11}$$

где $q_0 \in \mathbb{Z}$, а $q_1,\ q_2,\ \ldots,\ q_n,\ \ldots \in \mathbb{N}$, называется *бесконечной цепной дробью.*

О п р е д е л е н и е 4. *Подходящей дробью* $\dfrac{P_n}{Q_n}$ к бесконечной цепной дроби (11) называется конечная цепная дробь

$$\frac{P_n}{Q_n} = q_0 + \cfrac{1}{q_1 + \ddots + \cfrac{1}{q_n}}. \tag{12}$$

О п р е д е л е н и е 5. Бесконечная дробь (11) называется *сходящейся*, если существует предел ее подходящих дробей, т.е.

$$\lim_{n\to\infty}\frac{P_n}{Q_n}.$$

О п р е д е л е н и е 6. *Величиной бесконечной сходящейся цепной дроби* (11) называется предел ее подходящих дробей, т.е. число $\alpha\in\mathbb{R}$, такое, что $\lim\limits_{n\to\infty}\dfrac{P_n}{Q_n}=\alpha$.

Свойства подходящих дробей, их числителей и знаменателей, сформулированные в теоремах 3–9, справедливы и для бесконечных цепных дробей. Действительно, как бы велико ни было n, подходящие дроби

$$\frac{P_0}{Q_0};\ \frac{P_1}{Q_1};\ \frac{P_2}{Q_2};\ \ldots;\ \frac{P_n}{Q_n}$$

к бесконечной дроби (11) являются вместе с тем подходящими дробями к конечной цепной дроби

$$q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_n+\cfrac{1}{q_{n+1}}}}}},$$

так что утверждения теорем 3–9 верны для всех n.

Докажем некоторые свойства подходящих дробей, которые имеют место для бесконечных цепных дробей.

Т е о р е м а 11. *При увеличении номера n знаменатели Q_n бесконечной цепной дроби неограниченно возрастают.*

Д о к а з а т е л ь с т в о. Поскольку в бесконечной цепной дроби $q_n \geqslant 1$ при всех $n \geqslant 1$, то, согласно сделанному выше замечанию результат теоремы 4 распространяется на любое множество значений n, так что

$$1 = Q_0 \leqslant Q_1 < Q_2 < \dots .$$

Так как $Q_n \in \mathbb{Z}$, то при $n > 1$ каждое Q_n по крайней мере на единицу больше предыдущего, т.е. $Q_n \to \infty$. Теорема доказана.

Т е о р е м а 12. *Расстояния между соседними подходящими дробями монотонно уменьшаются с увеличением номера и стремятся к нулю.*

Д о к а з а т е л ь с т в о. Согласно теоремам 4 и 5 имеем:

$$\left|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right| = \frac{1}{Q_{n+1}Q_n} < \frac{1}{Q_{n-1}Q_n} = \left|\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right| .$$

Но так как, согласно предыдущей теореме $Q_n \to \infty$, то

$$\left|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right| = \frac{1}{Q_{n+1}Q_n} \to 0 .$$

Теорема доказана.

Т е о р е м а 13. *Подходящие дроби с четными и нечетными номерами образуют систему концов вложенных друг в друга интервалов.*

Д о к а з а т е л ь с т в о. В теоремах 7 и 9 мы показали, что четные подходящие дроби образуют возрастающую последовательность, а нечетные подходящие дроби — убыва-

ющую последовательность, и при этом любая четная дробь меньше любой нечетной дроби.

Так как все это справедливо для любого числа подходящих дробей, то

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \ldots < \frac{P_5}{Q_5} < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}.$$

Докажем теорему, утверждающую, что рассматриваемые нами бесконечные цепные дроби всегда сходятся, и, следовательно, имеют определенную величину.

Т е о р е м а 14. *Любая бесконечная цепная дробь сходится.*

Д о к а з а т е л ь с т в о. Пусть дана бесконечная цепная дробь (12). В предыдущей теореме мы установили, что подходящие дроби с четными и нечетными номерами являются левыми и правыми концами системы вложенных друг в друга интервалов. Согласно теореме 12 имеем:

$$\left| \frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}} \right| \to 0\,,$$

поэтому длины интервалов:

$$\left(\frac{P_0}{Q_0}, \frac{P_1}{Q_1}\right), \left(\frac{P_2}{Q_2}, \frac{P_3}{Q_3}\right), \ \ldots$$

стремятся к нулю при увеличении n.

Согласно теореме о вложенных интервалах (см. курс математического анализа) левые и правые концы такой системы вложенных друг в друга интервалов, длины которых стремятся к нулю, имеют общий предел, представляющий собой некоторое действительное число α, такое, что

$$\lim_{k\to\infty} \frac{P_k}{Q_k} = \alpha\,.$$

Теорема доказана.

З а м е ч а н и е. Из доказательства следует, что величина бесконечной цепной дроби больше любой четной подходящей дроби и меньше любой нечетной подходящей дроби, т.е.

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \ldots < \alpha < \ldots < \frac{P_5}{Q_5} < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}.$$

О п р е д е л е н и е 7. Пусть $\alpha = [q_0;\ q_1,\ q_2,\ \ldots]$. *Полными частными* в разложении α будем называть величины $\alpha_0,\ \alpha_1,\ \alpha_2,\ \ldots$, определенные равенствами:

$$\alpha = [q_0;\ q_1,\ q_2,\ \ldots,\ q_k,\ \alpha_{k+1}] \text{ при } k \geqslant 0,$$

$$\alpha = \alpha_0 \text{ при } k = -1.$$

Т е о р е м а 15. *Пусть* $\alpha = [q_0;\ q_1,\ q_2,\ \ldots]$, α_{k+1} — *полное частное в разложении* α. *Тогда*

$$\alpha = \frac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}}$$

и

$$\alpha_{k+1} = \frac{P_{k-1} - \alpha Q_{k-1}}{\alpha Q_k - P_k},$$

где $P_k,\ Q_k,\ P_{k-1},\ Q_{k-1}$ — *числители и знаменатели* k*-ой и* $(k-1)$*-ой подходящей дроби к* α.

Д о к а з а т е л ь с т в о. Сравним два выражения:

$$\frac{P_{k+1}}{Q_{k+1}} = [q_0;\ q_1,\ q_2,\ \ldots,\ q_k,\ q_{k+1}]$$

и

$$\alpha = [q_0;\ q_1,\ q_2,\ \ldots,\ q_k,\ \alpha_{k+1}].$$

Понятно, что если в первом выражении заменить q_{k+1} через α_{k+1}, то получим второе выражение. В силу теоремы 3 будем иметь:

$$\frac{P_{k+1}}{Q_{k+1}} = \frac{P_k q_{k+1} + P_{k-1}}{Q_k q_{k+1} + Q_{k-1}},$$

где P_k, Q_k, P_{k-1}, Q_{k-1} не зависят от значения неполных частных q_{k+1}.

Заменяя в этом равенстве q_{k+1} на α_{k+1}, получим:

$$\alpha = \frac{P_k \alpha_{k+1} + P_{k-1}}{Q_k \alpha_{k+1} + Q_{k-1}},$$

откуда, выразив α_{k+1}, придем к равенству:

$$\alpha_{k+1} = \frac{P_{k-1} - \alpha Q_{k-1}}{\alpha Q_k - P_k}.$$

Теорема доказана.

З а м е ч а н и е. Доказанная теорема будет иметь смысл при $k = 0$ и $k = 1$, если положить

$$P_{-1} = 1,\ Q_{-1} = 0,\ P_{-2} = 0,\ Q_{-2} = 1.$$

Действительно,

$$\alpha = q_0 + \frac{1}{\alpha_1} = \frac{q_0 \alpha_1 + 1}{\alpha_1} = \frac{P_0 \alpha_1 + 1}{Q_0 \alpha_1 + 0} \text{ и } \alpha = \frac{1 \cdot \alpha + 0}{0 \cdot \alpha + 1}.$$

В дальнейшем, рассматривая величины P_k, Q_k, при $k = -1$ и $k = -2$ будем всегда считать, что

$$P_{-1} = 1,\ Q_{-1} = 0,\ P_{-2} = 0,\ Q_{-2} = 1.$$

2. Разложение действительных чисел в цепные дроби.

О п р е д е л е н и е 8. *Разложением действительного числа α в цепную дробь* называется представление α

в виде $\alpha = [q_0;\ q_1,\ q_2,\ \ldots]$, где $q_0,\ q_1,\ q_2,\ \ldots$ — конечная или бесконечная последовательность целых чисел, такая, что при $i \geqslant 1$ все $q_i \geqslant 1$, а в случае конечного разложения последний элемент $q_k > 1$.

Т е о р е м а 16. *Пусть разложение α в цепную дробь имеет вид: $\alpha = [q_0;\ q_1,\ q_2,\ \ldots]$. Введем обозначение: $\alpha'_k = [q_k;\ q_{k+1},\ q_{k+2},\ \ldots]$. Тогда:*

1. $\alpha = [q_0;\ q_1,\ q_2,\ \ldots,\ q_{k-1},\ \alpha'_k]$, т.е. *$\alpha'_k = \alpha_k$ представляет собой k-ое полное частное в разложении α;*

2. $\forall k\ q_k = [\alpha_k]$.

Д о к а з а т е л ь с т в о.

1. Для конечной цепной дроби это равенство очевидно, поэтому рассмотрим случай бесконечной цепной дроби. Если предел подходящих дробей к бесконечной цепной дроби $[q_k;\ q_{k+1},\ q_{k+2},\ \ldots]$ равен α'_k, то $\alpha'_k > 1$ и согласно известным из курса математического анализа теоремам о пределе суммы и частного,

$$\lim_{s\to\infty}[q_0;\ q_1,\ q_2,\ \ldots,\ q_{k-1},\ q_k,\ q_{k+1},\ldots,\ q_{k+s}] =$$

$$= [q_0;\ q_1,\ q_2,\ \ldots,\ q_{k-1}] + \frac{1}{\lim\limits_{s\to\infty}[q_k,\ q_{k+1},\ldots,\ q_{k+s}]},$$

т.е., действительно, $\alpha = [q_0;\ q_1,\ q_2,\ \ldots,\ q_{k-1},\ \alpha'_k],\ \alpha'_k = \alpha_k$.

2. Если цепная дробь конечная и q_k — ее последний элемент, то $q_k = \alpha_k = [\alpha_k]$. Если же q_k не является последним элементом, то $\alpha_{k+1} = \alpha'_{k+1} = [q_{k+1};\ q_{k+2},\ q_{k+3},\ \ldots] > 1$, поэтому $0 < \dfrac{1}{\alpha_{k+1}} < 1$, и, как мы доказали в первой части, $\alpha_k = q_k + \dfrac{1}{\alpha_{k+1}}$, так что $q_k = [\alpha_k]$. Теорема доказана.

З а д а ч а 7. Найти величину цепной дроби:

$$\alpha = [1;\ 4,\ 1,\ 4,\ \ldots],$$

где все дальнейшие элементы равны последовательно 1 и 4.

Р е ш е н и е. Применим к условию задачи предыдущую теорему:

$$\alpha = [1;\ 4,\ \alpha] = 1 + \frac{1}{4 + \dfrac{1}{\alpha}} = 1 + \frac{\alpha}{4\alpha + 1} = \frac{5\alpha + 1}{4\alpha + 1},$$

откуда приходим к квадратному уравнению

$$4\alpha^2 - 4\alpha - 1 = 0,$$

решая которое, находим:

$$\alpha_{1,2} = \frac{1 \pm \sqrt{2}}{2}.$$

Но поскольку $\alpha > 0$, то

$$\alpha = \frac{1 + \sqrt{2}}{2}.$$

З а д а ч а 8. Найти величину цепной дроби:

$$\alpha = [2;\ 2,\ 2,\ 1,\ 2,\ 2,\ 2,\ 1,\ \ldots],$$

где все дальнейшие элементы последовательно принимают значения 2, 2, 2, 1.

Р е ш е н и е. Используя теоремы 15 и 16, получим:

$$\alpha = [2;\ 2,\ 2,\ 1,\ \alpha], \quad \alpha = \frac{P_3\alpha + P_2}{Q_3\alpha + Q_2}.$$

Составим вспомогательную таблицу подходящих дробей при $n = 0,\ 1,\ 2,\ 3,\ 4$:

k		0	1	2	3	4
q_k		2	2	2	1	α
P_k	1	2	5	12	17	$17\alpha + 12$
Q_k	0	1	2	5	7	$7\alpha + 5$

так что $\alpha = \dfrac{17\alpha + 12}{7\alpha + 5}$.

После элементарных преобразований:

$$7\alpha^2 - 12\alpha - 12 = 0.$$

Решая это квадратное уравнение и учитывая, что $\alpha > 0$, будем иметь:

$$\alpha = \frac{6 + 2\sqrt{30}}{7}.$$

Докажем теперь теорему существования и единственности разложения всякого иррационального числа в бесконечную цепную дробь (для рациональных чисел аналогичную теорему мы доказали в §1 этой главы).

Т е о р е м а 17. *Для любого иррационального числа α существует разложение в бесконечную цепную дробь, причем последняя определяется единственным образом.*

Д о к а з а т е л ь с т в о.

С у щ е с т в о в а н и е. Обозначим через q_0 целую часть α, а через α_1 — величину, обратную дробной части α, т.е. возьмем $\alpha_1 = \dfrac{1}{\alpha - q_0}$, так что $\alpha = q_0 + \dfrac{1}{\alpha_1}$.

Поскольку α — иррационально, $q_0 \neq \alpha$ и α_1 также иррациональное число, причем $\alpha_1 > 1$.

Таким образом, мы установили, что для любого иррационального числа α можно найти целое число $q_0 = [\alpha]$ и иррациональное число α_1, такие, что $\alpha = q_0 + \dfrac{1}{\alpha_1}$. Находя аналогично для числа α_1 числа $q_1 = [\alpha_1]$ и $\alpha_2 > 1$, для α_2 числа $q_2 = [\alpha_2]$ и $\alpha_3 > 1$ и т.д., получим:

$$\begin{cases} \alpha = q_0 + \dfrac{1}{\alpha_1} & q_0 = [\alpha] \\ \alpha_1 = q_1 + \dfrac{1}{\alpha_2} & q_1 = [\alpha_1] \\ \alpha_2 = q_2 + \dfrac{1}{\alpha_3} & q_2 = [\alpha_2] \\ \ldots \quad \ldots \quad \ldots \quad \ldots & \ldots \quad \ldots \quad \ldots \\ \alpha_k = q_k + \dfrac{1}{\alpha_{k+1}} & q_k = [\alpha_k] \\ \ldots \quad \ldots \quad \ldots \quad \ldots & \ldots \quad \ldots \quad \ldots, \end{cases} \tag{13}$$

где при $k \geqslant 1$ все иррациональные числа $\alpha_k > 1$ и, таким образом, при всех таких k числа $q_k = [\alpha_k] \geqslant 1$.

Числа $q_0,\ q_1,\ q_2,\ \ldots$ образуют бесконечную последовательность целых чисел и, поскольку при $k \geqslant 1\ q_k \geqslant 1$, мы можем взять эти числа в качестве элементов, составить бесконечную цепную дробь $[q_0;\ q_1,\ q_2,\ \ldots]$, которая в силу теоремы 14 сходится.

Докажем, что величина этой цепной дроби равна нашему числу α. Из равенств (13) получаем

$$\alpha = [q_0;\ q_1,\ q_2,\ \ldots,\ q_k,\ \alpha_{k+1}],$$

так что согласно теореме 15 имеем:

$$\alpha = \frac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}}$$

и

$$\left|\alpha - \frac{P_k}{Q_k}\right| = \left|\frac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}} - \frac{P_k}{Q_k}\right| =$$

$$= \left|\frac{Q_k(P_k\alpha_{k+1} + P_{k-1}) - P_k(Q_k\alpha_{k+1} + Q_{k-1})}{Q_k(Q_k\alpha_{k+1} + Q_{k-1})}\right| =$$

$$= \left|\frac{Q_kP_k\alpha_{k+1} + P_{k-1}Q_k - P_kQ_k\alpha_{k+1} - P_kQ_{k-1}}{Q_k(Q_k\alpha_{k+1} + Q_{k-1})}\right| =$$

$$= \left|\frac{(-1)^k}{Q_k(Q_k\alpha_{k+1} + Q_{k-1})}\right| = \frac{1}{Q_k(Q_k\alpha_{k+1} + Q_{k-1})} <$$

$$< \frac{1}{Q_k^2\alpha_{k+1}} < \frac{1}{Q_k^2}.$$

Поскольку $Q_k \to \infty$ (см. теорему 12), величина $\left|\alpha - \dfrac{P_k}{Q_k}\right|$ при увеличении k становится меньше любого сколь угодно малого наперед заданного положительного числа ε , т.е.

$$\lim_{k\to\infty} \frac{P_k}{Q_k} = \alpha.$$

Мы видим, таким образом, что для заданного иррационального числа α имеется алгоритм, позволяющий строить цепную дробь, равную α.

Легко показать, что для рациональных α алгоритм (13) совпадает с алгоритмом (6) и (6′), причем при рациональном α все α_k также рациональны и процесс заканчивается, как только α_k становится целым числом.

Единственность. Нужно доказать, что представление любого иррационального числа в виде бесконечной цепной дроби единственно.

Предположим противное, т.е. пусть возможны два представления числа α в виде бесконечной цепной дроби:

$$\alpha = [a_0;\ a_1,\ a_2,\ \ldots] = [b_0;\ b_1,\ b_2,\ \ldots],$$

где a_i и b_i — целые числа, причем при $i \geqslant 1$ все a_i и b_i положительны.

Допустим, что эти две бесконечные цепные дроби отличаются хотя бы одним элементом и обозначим через k первый по порядку номер, такой, что $a_k \neq b_k$, т.е. предположим, что

$$a_0 = b_0,\ a_1 = b_1,\ \ldots,\ a_{k-1} = b_{k-1},\ a_k \neq b_k.$$

Обозначим

$$\alpha_k = [a_k;\ a_{k+1};\ a_{k+2},\ \ldots],$$

$$\beta_k = [b_k;\ b_{k+1};\ b_{k+2},\ \ldots].$$

Из равенства (см. теорему 16_1)

$$\alpha = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1},\ \alpha_k] = [b_0;\ b_1,\ b_2,\ \ldots,\ b_{k-1},\ \beta_k]$$

получаем $\alpha_k = \beta_k$, но тогда согласно теореме 16_2 имеем:

$$a_k = [\alpha_k] = [\beta_k] = b_k,$$

что противоречит условию $a_k \neq b_k$. Полученное противоречие говорит о том, что разложение иррационального числа в бесконечную цепную дробь единственно. Теорема полностью доказана.

З а м е ч а н и е. Из теорем 14 и 17, а также замечания к теоремам 1 и 2 следует, что иррациональные числа и только они могут быть представлены бесконечными цепными дробями.

Сделаем важный вывод: *между множеством действительных чисел* $\mathbb{R}$ *и множеством всех цепных дробей*

установлено взаимно-однозначное соответствие (биекция). При этом рациональным числам соответствуют конечные цепные дроби, а иррациональным числам — бесконечные цепные дроби.

В дальнейшем, когда действительное число α разложено в цепную дробь

$$[q_0;\ q_1,\ q_2,\ \ldots]$$

(конечную или бесконечную), мы будем подходящие дроби $\dfrac{P_k}{Q_k}$ к этой цепной дроби называть для краткости подходящими дробями к числу α.

З а д а ч а 9. Разложить в цепную дробь число $\alpha = \sqrt{2}$.

Р е ш е н и е. Находим:

$$q_0 = \left[\sqrt{2}\right] = 1, \quad \alpha_1 = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{1} = \sqrt{2}+1,$$

$$q_1 = \left[\sqrt{2}+1\right] = 2, \quad \alpha_2 = \frac{1}{(\sqrt{2}+1)-2} = \frac{1}{\sqrt{2}-1}.$$

Поскольку $\alpha_2 = \alpha_1$, будем иметь $q_2 = [\alpha_2] = [\alpha_1] = q_1 = 2$, так что $\alpha_3 = \alpha_2$ и т.д. В последовательных равенствах (13) будет:

$$\alpha_1 = \alpha_2 = \alpha_3 = \ldots; \quad q_0 = 1;\ q_1 = q_2 = q_3 = \ldots = 2,$$

т.е.

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}},$$

или короче: $\sqrt{2} = [1;\ 2,\ 2,\ 2,\ 2,\ \ldots]$.

З а д а ч а 10. Найти первые четыре элемента разложения в цепную дробь числа $\pi = 3{,}14159265\ldots$

Р е ш е н и е. Находим:

$$q_0 = [\pi] = 3; \quad \alpha_1 = \frac{1}{0{,}14159265\ldots}; \quad q_1 = [\alpha_1] = 7;$$

$$\alpha_2 = \frac{1}{\alpha_1 - q_1} = \frac{0{,}14159265\ldots}{0{,}00885145\ldots}; \quad q_2 = [\alpha_2] = 15;$$

$$\alpha_3 = \frac{1}{\alpha_2 - q_2} = \frac{0{,}00885145\ldots}{0{,}00882090\ldots}; \quad q_3 = [\alpha_3] = 1.$$

Таким образом,

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \ddots}}} = [3;\ 7,\ 15,\ 1,\ \ldots].$$

§3. Приближение действительных чисел рациональными числами

1. Приближение действительных чисел подходящими дробями. Применение иррациональных чисел на практике обычно осуществляется заменой данного иррационального числа некоторым рациональным числом, мало отличающимся в пределах требуемой точности от этого иррационального числа. При этом обычно стараются выбрать рациональное число возможно простым, т.е. в виде десятичной дроби с небольшим числом знаков после запятой или в

виде обыкновенной дроби со сравнительно небольшим знаменателем.

Для громоздких рациональных чисел, т.е. чисел с большими знаменателями, также иногда возникают задачи, связанные с необходимостью отыскания хороших рациональных приближений, понимая под этим отыскание рациональных чисел со сравнительно небольшими знаменателями, мало отличающимися от данных чисел.

Цепные дроби дают очень удобный способ для решения задач такого рода. С помощью подходящих дробей удается заменять действительные числа рациональными дробями так, что ошибка от такой замены мала по сравнению со знаменателями этих рациональных чисел.

Т е о р е м а 18. *Для любых двух соседних подходящих дробей* $\dfrac{P_k}{Q_k}$ *и* $\dfrac{P_{k+1}}{Q_{k+1}}$ *к действительному числу* α *имеет место неравенство:*

$$\left|\alpha - \frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_k Q_{k+1}}, \tag{14}$$

и если $\alpha \neq \dfrac{P_{k+1}}{Q_{k+1}}$, то

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k Q_{k+1}}.$$

Д о к а з а т е л ь с т в о. Если $\alpha \neq \dfrac{P_{k+1}}{Q_{k+1}}$, то подходящие дроби $\dfrac{P_k}{Q_k}$ и $\dfrac{P_{k+1}}{Q_{k+1}}$, из которых одна четная, а другая нечетная, лежат по разные стороны от α (см. теорему 10 и замечание к теореме 14), поэтому расстояние от α до лю-

бой из них меньше длины интервала, образованного этими двумя подходящими дробями, т.е.

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k Q_{k+1}}.$$

Если $\alpha = \dfrac{P_{k+1}}{Q_{k+1}}$, то $\left|\alpha - \dfrac{P_k}{Q_k}\right| = \dfrac{1}{Q_k Q_{k+1}}$. Теорема доказана.

Т е о р е м а 19. *Для любой подходящей дроби* $\dfrac{P_k}{Q_k}$ *к действительному числу* α *справедливо неравенство:*

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k^2}.$$

Д о к а з а т е л ь с т в о. Если $\alpha = \dfrac{P_k}{Q_k}$, то вышеприведенное неравенство очевидно. Пусть $\alpha \neq \dfrac{P_k}{Q_k}$, т.е. существует подходящая дробь $\dfrac{P_{k+1}}{Q_{k+1}}$. При $k > 0$ $Q_k < Q_{k+1}$, поэтому, согласно предыдущей теореме имеем:

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{Q_k Q_{k+1}} < \frac{1}{Q_k^2}.$$

Если $k = 0$ и $\alpha = [q_0;\ q_1,\ q_2,\ \ldots]$, то

$$\left|\alpha - \frac{P_0}{Q_0}\right| = \frac{1}{[q_1;\ q_2,\ q_3,\ \ldots]} < 1 = \frac{1}{Q_0^2}.$$

Теорема доказана.

Т е о р е м а 20. *Если* $\alpha \neq \dfrac{P_k}{Q_k}$, *то*

$$\left|\alpha - \frac{P_k}{Q_k}\right| > \frac{1}{Q_k(Q_{k+1} + Q_k)}.$$

Д о к а з а т е л ь с т в о. Рассмотрим сначала случай, когда для α существует подходящая дробь $\dfrac{P_{k+2}}{Q_{k+2}}$. Тогда при $\alpha \neq \dfrac{P_{k+2}}{Q_{k+2}}$ подходящие дроби $\dfrac{P_k}{Q_k}$ и $\dfrac{P_{k+2}}{Q_{k+2}}$ находятся по одну сторону от числа α (см. теорему 10 и замечание к теореме 14), поэтому

$$\left|\alpha - \frac{P_k}{Q_k}\right| > \left|\frac{P_{k+2}}{Q_{k+2}} - \frac{P_k}{Q_k}\right| = \frac{\left|P_{k+2}Q_k - P_kQ_{k+2}\right|}{Q_kQ_{k+2}} =$$

$$= \frac{\left|(P_{k+1}q_{k+2} + P_k)Q_k - (Q_{k+1}q_{k+2} + Q_k)P_k\right|}{Q_k(Q_{k+1}q_{k+2} + Q_k)} =$$

$$= \frac{q_{k+2}(P_{k+1}Q_k - Q_{k+1}P_k)}{Q_k(Q_{k+1}q_{k+2} + Q_k)} = \frac{\left|q_{k+2}\cdot(-1)^{k+2}\right|}{Q_k(Q_{k+1}q_{k+2} + Q_k)} =$$

$$= \frac{q_{k+2}}{Q_k(Q_{k+1}q_{k+2} + Q_k)} \geqslant \frac{q_{k+2}}{Q_k(Q_{k+1}q_{k+2} + Q_kq_{k+2})} =$$

$$= \frac{1}{Q_k(Q_{k+1} + Q_k)}.$$

При $\alpha = \dfrac{P_{k+2}}{Q_{k+2}}$ будет $q_{k+2} > 1$, так что

$$\left|\alpha - \frac{P_k}{Q_k}\right| = \left|\frac{P_{k+2}}{Q_{k+2}} - \frac{P_k}{Q_k}\right| = \frac{q_{k+2}}{Q_k(Q_{k+1}q_{k+2} + Q_k)} >$$

$$> \frac{q_{k+2}}{Q_k(Q_{k+1}q_{k+2} + Q_kq_{k+2})} = \frac{1}{Q_k(Q_{k+1} + Q_k)}.$$

Если же $\dfrac{P_{k+1}}{Q_{k+1}}$ — последняя подходящая дробь, т.е. $\alpha =$

$= \dfrac{P_{k+1}}{Q_{k+1}}$, то

$$\left|\alpha - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k Q_{k+1}} > \frac{1}{Q_k(Q_{k+1} + Q_k)}.$$

Теорема доказана.

З а м е ч а н и е. Теоремы 18 и 20 дают оценки приближения любого действительного числа подходящей дробью $\dfrac{P_k}{Q_k}$. Так как $\forall k\ Q_k \leqslant Q_{k+1}$, то можно записать:

$$\frac{1}{2Q_k Q_{k+1}} < \left|\alpha - \frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_k Q_{k+1}},$$

т.е. дробь $\dfrac{1}{Q_k Q_{k+1}}$ с точностью до множителя $\theta \in \left(\dfrac{1}{2};\ 1\right]$ определяет порядок приближения α подходящей дробью с номером k.

З а д а ч а 11. Заменить рациональное число

$$\frac{a}{b} = \frac{245}{83}$$

такой подходящей дробью, чтобы полученная при этом погрешность не превышала 0,001.

Р е ш е н и е.

1. Разлагаем число $\dfrac{245}{83}$ в цепную дробь:

$$\frac{245}{83} = [2;\ 1,\ 19,\ 1,\ 3]$$

(проверьте это самостоятельно!).

2. Находим все подходящие дроби, последовательно заполнив таблицу:

k		0	1	2	3	4
q_k		2	1	19	1	3
P_k	1	2	3	59	62	245
Q_k	0	1	1	20	21	83

3. Начнем проверять выполнение неравенства (14) для подходящих дробей, например, с порядка $k = 2$:

$$\left|\frac{245}{83} - \frac{59}{20}\right| < \frac{1}{20 \cdot 21} > \frac{1}{1000}.$$

Следовательно, дробь $\dfrac{P_2}{Q_2}$ не подходит.

$$\left|\frac{245}{83} - \frac{62}{21}\right| = \frac{1}{21 \cdot 83} < \frac{1}{1000},$$

поэтому искомая подходящая дробь $\dfrac{P_3}{Q_3} = \dfrac{62}{21}$.

З а д а ч а 12. Найти подходящую дробь к числу $2 + \sqrt{5}$, отличающуюся от этой иррациональности меньше, чем на 0,00001.

Р е ш е н и е.

1. Представим число $2 + \sqrt{5}$ в виде бесконечной цепной дроби: $2 + \sqrt{5} = [4;\ 4,\ 4,\ 4,\ \ldots]$ (проверьте самостоятельно!).

2. Составим вспомогательную таблицу подходящих дробей:

k		0	1	2	3	4	5	...
q_k		4	4	4	4	4	4	...
P_k	1	4	17	72	305	1292	5473	...
Q_k	0	1	4	17	72	305	1292	...

3. Начнем проверять выполнение неравенства (14) для подходящих дробей, например, с порядка $k = 3$:

$$\left|(2+\sqrt{5}) - \frac{305}{72}\right| < \frac{1}{72 \cdot 305} > \frac{1}{100000}.$$

Следовательно, дробь $\dfrac{P_3}{Q_3}$ не подходит.

$$\left|(2+\sqrt{5}) - \frac{1292}{305}\right| < \frac{1}{305 \cdot 1292} < \frac{1}{100000},$$

поэтому искомая подходящая дробь $\dfrac{P_4}{Q_4} = \dfrac{1292}{305}$.

Докажем теперь, что каждая следующая подходящая дробь всегда ближе к рассматриваемому действительному числу α, чем предыдущая.

Т е о р е м а 21. *Для любых двух соседних подходящих дробей* $\dfrac{P_{k-1}}{Q_{k-1}}$ *и* $\dfrac{P_k}{Q_k}$ *к действительному числу* α *имеем:*

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \left|\alpha - \frac{P_{k-1}}{Q_{k-1}}\right|. \tag{15}$$

Д о к а з а т е л ь с т в о. Как и в теореме 17, согласуясь с теоремой 15, при $\alpha \neq \dfrac{P_k}{Q_k}$ получаем:

$$\left|\alpha - \frac{P_k}{Q_k}\right| = \left|\frac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}} - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k(Q_k\alpha_{k+1} + Q_{k-1})},$$

$$\left|\alpha - \frac{P_{k-1}}{Q_{k-1}}\right| = \left|\frac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}} - \frac{P_{k-1}}{Q_{k-1}}\right| = \frac{\alpha_{k+1}}{Q_k(Q_k\alpha_{k+1} + Q_{k-1})}.$$

Но так как $\alpha_{k+1} > 1$ и $Q_k \geqslant Q_{k-1}$, то

$$\frac{1}{Q_k(Q_k\alpha_{k+1} + Q_{k-1})} < \frac{\alpha_{k+1}}{Q_{k-1}(Q_k\alpha_{k+1} + Q_{k-1})},$$

откуда и

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \left|\alpha - \frac{P_{k-1}}{Q_{k-1}}\right|.$$

При $\alpha = \dfrac{P_k}{Q_k}$ неравенство (15), очевидно, выполняется. Теорема доказана.

2. Теорема Дирихле. Закономерность возможного приближения любого действительного числа α рациональной дробью, независимо от того или иного ее вида, выражает следующая важная теорема, которая носит имя Дирихле.

Т е о р е м а 22 (Д и р и х л е). *Пусть даны действительные числа α и $\tau \geqslant 1$. Тогда существует несократимая дробь $\dfrac{a}{b}$, для которой*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}, \quad 0 < b \leqslant \tau.$$

Д о к а з а т е л ь с т в о. Пусть $\dfrac{P_k}{Q_k}$ — подходящая дробь числа α. Выберем наибольший из знаменателей Q_k, не превышающий τ, т.е. найдем наибольшее k, чтобы выполнялось неравенство $Q_k \leqslant \tau$ и положим $\dfrac{a}{b} = \dfrac{P_k}{Q_k}$.

Не останавливаясь на тривиальном случае, когда $\alpha = \dfrac{P_k}{Q_k}$, имеем $Q_k \leqslant \tau < Q_{k+1}$, поэтому

$$\left|\alpha - \frac{a}{b}\right| = \left|\alpha - \frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_kQ_{k+1}} < \frac{1}{b\tau}.$$

Теорема доказана.

З а д а ч а 13. Найти рациональное приближение $\frac{a}{b}$ к $\sqrt{5}$ с точностью до $\frac{1}{1000b}$.

Р е ш е н и е. По теореме Дирихле такую дробь можно найти среди дробей со знаменателями, меньшими, чем 1000.

1. Разложим $\sqrt{5}$ в цепную дробь: $\sqrt{5} = [2;\ 4,\ 4,\ 4,\ \ldots]$
2. Найдем подходящие дроби, заполнив таблицу:

k		0	1	2	3	4	5	...
q_k		2	4	4	4	4	4	...
P_k	1	2	9	38	161	682	2889	...
Q_k	0	1	4	17	72	305	1292	...

3. Наибольшим знаменателем, меньшим чем 1000, является $Q_4 = 305$. Искомая дробь равна $\frac{682}{305}$, при этом

$$\left|\sqrt{5} - \frac{682}{305}\right| < \frac{1}{1000 \cdot 305}.$$

3. Подходящие дроби как наилучшие приближения. Подходящие дроби в определенном смысле, который мы поясним в этом пункте, являются наилучшими приближениями к действительным числам.

Говоря о наилучшем приближении, мы понимаем под этим наилучшее приближение по сравнению не со всеми другими рациональными числами, а только по сравнению с дробями, у которых знаменатель меньше, чем у данной дроби, или равен ему.

О п р е д е л е н и е 9. Рациональная дробь $\frac{a}{b}$ называется *наилучшим приближением* к действительному числу α, если не существует ни одной рациональной дроби $\frac{p}{q}$ со знаменателем $q \leqslant b$, которая была бы ближе к α, чем $\frac{a}{b}$.

Из определения следует, что дробь $\frac{a}{b}$ является наилучшим приближением к α, если для любой другой рациональной дроби $\frac{p}{q}$, такой, что

$$\left|\alpha - \frac{p}{q}\right| < \left|\alpha - \frac{a}{b}\right|,$$

будем иметь $q > b$.

Раскроем геометрический смысл определения. Если взять на числовой прямой точку α и интервал

$$\left(\alpha - \frac{a}{b};\ \alpha + \frac{a}{b}\right),$$

то все рациональные дроби из этого интервала имеют знаменатели, большие чем b.

Таким образом, если $\frac{a}{b}$ — наилучшее приближение к α, то рациональные дроби со знаменателями $\leqslant b$ лежат вне этого интервала или совпадают с одним из его концов.

Приведем некоторые примеры:

а) $\frac{5}{2}$ является наилучшим приближением к числу $e = 2{,}718281828\ldots$, так как среди рациональных дробей со знаменателями 1 и 2 нет ни одной, которая была бы ближе

к e, чем $\frac{5}{2}$, т.е. ближе к e, чем $\frac{5}{2}$, могут быть только дроби $\frac{a}{b}$, где $b > 2$.

б) $\frac{10}{7}$ не есть наилучшее приближение к $\sqrt{2} = 1{,}4142\ldots$, т.к. дробь $\frac{7}{5} = 1{,}4$ со знаменателем, меньшим, чем у $\frac{10}{7}$, ближе к $\sqrt{2}$, чем $\frac{10}{7} = 1,428\ldots$.

Рассмотрим вопрос об отыскании наилучших приближений к действительным числам.

Т е о р е м а 23. *Если интервал* $\left(\frac{a}{b};\ \frac{c}{d}\right)$ *образован двумя рациональными дробями, такими, что* $bc - ad = 1$, *то:*

1) *любая рациональная дробь из этого интервала имеет знаменатель, больший чем* b *и* d;

2) *для любого действительного числа* α, *принадлежащему этому интервалу, хотя бы одна из дробей* $\frac{a}{b}$ *или* $\frac{c}{d}$, *а именно ближайшая к* α, *является наилучшим приближением.*

Д о к а з а т е л ь с т в о.

1) Подберем рациональную дробь $\frac{p}{q}$ из расчета, чтобы

$$\frac{a}{b} < \frac{p}{q} < \frac{c}{d}.$$

Имеем: $bc - ad = 1$, тогда, поскольку $a,\ p \in \mathbb{Z}$ и $b,\ q \in \mathbb{N}$, получаем $bp - aq > 0$, откуда $bp - aq \geqslant 1$, а, следовательно,

$$\frac{p}{q} - \frac{a}{b} = \frac{bp - aq}{bq} \geqslant \frac{1}{bq}. \tag{16}$$

С другой стороны, так как $\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$, то

$$\frac{p}{q} - \frac{a}{b} < \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd} = \frac{1}{bd}, \tag{17}$$

поэтому, сравнивая (16) и (17), приходим к неравенству $\frac{1}{bq} < \frac{1}{bd}$, т.е. $q > d$.

Аналогично, рассматривая вместо $bp - aq$ выражение $cq - dp$ и вместо $\frac{p}{q} - \frac{a}{b}$ разность $\frac{c}{d} - \frac{p}{q}$, можно доказать, что $q > b$.

2) Пусть $\frac{a}{b} < \alpha < \frac{c}{d}$, $bc - ad = 1$. Если $\frac{a}{b}$ ближе к α, чем $\frac{c}{d}$, то $\frac{a}{b}$ — наилучшее приближение к α.

Действительно, любая рациональная дробь $\frac{p}{q}$, лежащая ближе к α, чем $\frac{a}{b}$, должна принадлежать интервалу $\left(\frac{a}{b}; \frac{c}{d}\right)$ и, следовательно, согласно первой части теоремы для нее будет $q > b$. Таким образом, любая дробь, которая ближе к α, чем $\frac{a}{b}$, имеет знаменатель, больший чем b, т.е. $\frac{a}{b}$ — наилучшее приближение к α.

Если $\frac{c}{d}$ ближе к α, чем $\frac{a}{b}$, то аналогично получаем, что $\frac{c}{d}$ — наилучшее приближение к α, а если числа $\frac{a}{b}$ и $\frac{c}{d}$ ле-

жат на равных расстояниях от α, то обе дроби являются наилучшими приближениями. Теорема доказана.

З а м е ч а н и е. Вообще говоря, оба конца интервала $\left(\frac{a}{b};\ \frac{c}{d}\right)$ могут быть одновременно наилучшими приближениями к α и тогда, когда расстояния от α до концов интервала не равны. Это подтверждает следующая теорема.

Т е о р е м а 24. *При $k \geqslant 1$ любая подходящая дробь $\frac{P_k}{Q_k}$ к действительному числу α является наилучшим приближением.*

Д о к а з а т е л ь с т в о. При $\alpha \neq \frac{P_k}{Q_k}$ α заключено в интервале $\left(\frac{P_k}{Q_k};\ \frac{P_{k-1}}{Q_{k-1}}\right)$, причем, учитывая формулы (10), $P_kQ_{k-1} - P_{k-1}Q_k = 1$, если k нечетно и $P_{k-1}Q_k - P_kQ_{k-1} = 1$, если k четно.

Согласно предыдущей теореме ближайшая к α из двух дробей $\frac{P_k}{Q_k}$ и $\frac{P_{k-1}}{Q_{k-1}}$, а таковой является $\frac{P_k}{Q_k}$ (см. теорему 21), является наилучшим приближением.

При $k = 0$ $Q_0 = 1$ и $\frac{P_0}{Q_0} = P_0 = [\alpha]$ не всегда является наилучшим приближением, так как $\frac{P_0 + 1}{Q_0} = [\alpha] + 1$ может быть ближе к α, чем $\frac{P_0}{Q_0}$. Теорема доказана.

З а м е ч а н и е. Обратная теорема в общем случае неверна, т.е. встречаются дроби, которые не служат подходящими к числу α и, тем не менее, являются наилучшими приближениями числа α. Например, дроби $\frac{19}{6}$, $\frac{16}{5}$ и $\frac{13}{4}$ явля-

ются наилучшими приближениями числа π, но не являются подходящими дробями к числу π. Поэтому доказанная теорема не означает, что наилучшими приближениями к действительному числу α всегда являются подходящие дроби к α.

Пример. Дробь $\dfrac{5473}{1292}$, найденная нами (см. задачу 12) в качестве хорошего приближения числа $2+\sqrt{5}$, является согласно последней теореме наилучшим приближением, т.е. ни одна дробь со знаменателем, не превосходящим 1292, не может быть ближе к $2+\sqrt{5}$, чем $\dfrac{5473}{1292}$.

Существуют и другие методы, позволяющие находить достаточно хорошие приближения к действительным числам.

§4. Квадратичные иррациональности и периодические цепные дроби

1. Разложение квадратичных иррациональностей в цепные дроби. Установив взаимно-однозначное соответствие между множеством действительных чисел $\mathbb{R}$ и множеством цепных дробей, мы разделили последние на два класса: конечные цепные дроби и бесконечные цепные дроби. Из множества бесконечных цепных дробей также можно выделить некоторый класс дробей, характеризующих иррациональные числа определенного вида. Это периодические цепные дроби.

Определение 10. Число α называется *квадратичной иррациональностью*, если α — иррациональный корень некоторого уравнения

$$ax^2+bx+c=0 \tag{18}$$

с целыми коэффициентами, не равными одновременно нулю. При таком α, очевидно, будет $a \neq 0,\ c \neq 0$.

Если коэффициенты $a,\ b,\ c$ взаимно просты, то дискриминант квадратного уравнения $D = b^2 - 4ac$ будем называть *дискриминантом числа* α.

Мы знаем, что корни квадратного уравнения (18) равны $x_1 = \dfrac{-b + \sqrt{b^2 - 4ac}}{2a}$ и $x_2 = \dfrac{-b - \sqrt{b^2 - 4ac}}{2a}$, поэтому любая квадратичная иррациональность будет иметь вид

$$\alpha = \frac{P + \sqrt{D}}{Q},$$

где P, Q целые, а D $(D > 1)$ — целое число, не являющееся точным квадратом. Второй корень уравнения (18) $\overline{\alpha} = \dfrac{P - \sqrt{D}}{Q}$ будем называть иррациональностью, *сопряженной* с α.

О п р е д е л е н и е 11. Цепная дробь $[q_0;\ q_1,\ q_2,\ \ldots]$ называется *периодической,* если периодической является последовательность элементов $q_0,\ q_1,\ q_2,\ \ldots$.

Если последовательность элементов чисто периодическая, то и соответствующая цепная дробь называется *чисто периодической,* в противном случае — *смешанной периодической.*

Длину периода последовательности $q_0,\ q_1,\ q_2,\ \ldots$ будем называть *длиной периода цепной дроби* $[q_0;\ q_1,\ q_2,\ \ldots]$. Если в разложении α после элементов $q_0,\ q_1,\ q_2,\ \ldots,\ q_{k-1}$ наступает периодическое повторение следующих t элементов $q_k,\ q_{k+1},\ q_{k+2},\ \ldots,\ q_{k+t-1}$, т.е. длина периода равна t $(t \geqslant 1)$, то будем записывать α в виде:

$$\alpha = [q_0;\ q_1,\ q_2,\ \ldots,\ q_{k-1},\ (q_k,\ q_{k+1},\ q_{k+2},\ \ldots,\ q_{k+t-1})].$$

В частности, в случае чисто периодического разложения, т.е. при $k = 0$, будем писать так:

$$\alpha = [(q_0;\ q_1,\ q_2,\ \ldots,\ q_{k-1})].$$

Т е о р е м а 25. *Для того, чтобы цепная дробь*

$$[q_0,\ q_1,\ q_2,\ \ldots] \tag{19}$$

была периодической с длиной периода t, необходимо и достаточно, чтобы при некотором k имело место равенство полных частных $\alpha_{k+t} = \alpha_k$.

Д о к а з а т е л ь с т в о. Имеем:

$$\alpha_k = [q_k;\ q_{k+1},\ q_{k+2},\ \ldots] \tag{20}$$

$$\alpha_{k+t} = [q_{k+t};\ q_{k+t+1},\ q_{k+t+2},\ \ldots] \tag{21}$$

Н е о б х о д и м о с т ь. Если правая часть в (19) представляет собой периодическую цепную дробь с длиной периода t, то существует такое k, что при всех $n \geqslant k$ $q_{n+t} = q_n$ и, следовательно, разложения (20) и (21) совпадают, т.е. $\alpha_{k+t} = \alpha_k$.

Д о с т а т о ч н о с т ь. Если $\alpha_{k+t} = \alpha_k$, где $k \geqslant 1$, то согласно единственности разложения действительного числа в цепную дробь (как конечную, так и бесконечную), разложения (20) и (21) одинаковы, т.е. $\forall n \geqslant k$ $q_{n+t} = q_n$ и, следовательно, дробь (19) периодическая с периодом t. Теорема доказана.

Оказывается, и это на первый взгляд кажется весьма неожиданным, что множество бесконечных периодических цепных дробей совпадает с множеством квадратичных иррациональностей. Этот результат получил известный французский математик Ж. Л. Лагранж в 1770 году.

2. Прямая и обратная теоремы Лагранжа.

Т е о р е м а 26 (Л а г р а н ж а). *Любая квадратичная иррациональность разлагается в бесконечную периодическую цепную дробь.*

Д о к а з а т е л ь с т в о. Пусть α — квадратичная иррациональность, т.е. α — иррациональное число, представляющее собой корень многочлена

$$f(x) = Ax^2 + Bx + C$$

с целыми коэффициентами. Подставляя в выражение $A\alpha^2 + B\alpha + C = 0 \quad \alpha = \dfrac{P_k\alpha_{k+1} + P_{k-1}}{Q_k\alpha_{k+1} + Q_{k-1}}$ (см. теорему 15) и приводя к общему знаменателю, получаем:

$$A(P_k\alpha_{k+1} + P_{k-1})^2 + B(P_k\alpha_{k+1} + P_{k-1})(Q_k\alpha_{k+1} + Q_{k-1}) + \\ + C(Q_k\alpha_{k+1} + Q_{k-1})^2 = 0.$$

Раскрыв скобки и перегруппировав слагаемые (выполните эти действия самостоятельно!), придем к квадратному уравнению относительно α_{k+1}:

$$A_k\alpha_{k+1}^2 + B_k\alpha_{k+1} + C_k = 0, \tag{22}$$

где

$$A_k = AP_k^2 + BP_kQ_k + CQ_k^2 = Q_k^2 \cdot f\left(\frac{P_k}{Q_k}\right);$$

$$B_k = 2AP_kP_{k-1} + B(P_kQ_{k-1} + P_{k-1}Q_k) + 2CQ_kQ_{k-1};$$

$$C_k = AP_{k-1}^2 + BP_{k-1}Q_{k-1} + CQ_{k-1}^2 = Q_k^2 \cdot f\left(\frac{P_{k-1}}{Q_{k-1}}\right)$$

— целые числа.

Непосредственным вычислением можно установить, что

$$B_k^2 - 4A_kC_k = B^2 - 4AC \tag{23}$$

(проверьте самостоятельно!). Таким образом, дискриминант уравнения (22) не меняется при увеличении k.

Докажем сначала, что A_k и C_k при достаточно большом k имеют противоположные знаки, а затем, пользуясь тождеством (23), докажем, что величины $A_k,\ B_k,\ C_k$ ограничены.

Дроби $\dfrac{P_k}{Q_k}$ и $\dfrac{P_{k-1}}{Q_{k-1}}$, как известно (см. теорему 14 и замечание к ней), находятся по разные стороны от α, причем при достаточно большом k сколь угодно мало отличаются от α.

Имеем: $f(\alpha) = 0$, но так как α — иррационально, то

$$f'(\alpha) = 2A\alpha + B \neq 0.$$

Значит, α является простым (не кратным) корнем уравнения $f(x) = 0$.

Известно, что в достаточно малой окрестности слева и справа от простого корня значения непрерывной функции, в данном случае многочлена $f(x) = Ax^2 + Bx + C$, имеют разные знаки (см. курс математического анализа), т.е. $A_k = Q_k^2 \cdot f\left(\dfrac{P_k}{Q_k}\right)$ и $C_k = Q_k^2 \cdot f\left(\dfrac{P_{k-1}}{Q_{k-1}}\right)$ при достаточно больших k противоположны по знаку, причем $f\left(\dfrac{P_k}{Q_k}\right)$ и $f\left(\dfrac{P_{k-1}}{Q_{k-1}}\right)$ и, следовательно, A_k и C_k не равны нулю.

Таким образом, при достаточно больших k произведение A_kC_k отрицательно и дискриминант уравнения (22) можно представить в виде суммы двух неотрицательных чисел: B_k^2 и $(-4A_kC_k)$. Так как $-4A_kC_k > 0$, $B_k^2 \geqslant 0$, то

$$0 \leqslant B_k^2 < B_k^2 - 4A_kC_k = B^2 - 4AC,$$

$$0 < -4A_kC_k \leqslant B_k^2 - 4A_kC_k = B^2 - 4AC,$$

т.е. величины B_k^2 и $(-4A_kC_k)$ ограничены. Из ограниченности B_k^2 следует ограниченность $\left|B_k\right|$, а из ограниченности $(-4A_kC_k)$, поскольку $(A_k \neq 0)\ \ \&\ \ (C_k \neq 0)$, следует ограниченность $\left|A_k\right|$ и $\left|C_k\right|$.

Другими словами, существуют две постоянные M и N, такие, что выполняются неравенства:

$$M < A_k < N, \quad M < B_k < N, \quad M < C_k < N,$$

а отсюда, так как $A_k,\ B_k,\ C_k \in \mathbb{Z}$, следует, что среди уравнений (22) при безграничном увеличении k существует только конечное число различных уравнений. Каждое квадратное уравнение в нашем случае имеет два корня, поэтому и среди корней уравнений (22) существует только конечное число различных, а значит, среди величин

$$\alpha = \alpha_0,\ \alpha_1,\ \alpha_2, \ldots \tag{24}$$

имеется только конечное число различных, следовательно, среди чисел (24) найдутся хотя бы два одинаковых, т.е. найдется α_s, равное некоторому последующему α_{s+t}. Равенство $\alpha_s = \alpha_{s+t}$ показывает, что разложение α в цепную дробь периодическое, и, таким образом, теорема доказана.

Т е о р е м а 27 (о б р а т н а я к т е о р е м е Л а г р а н ж а). *Величина любой бесконечной периодической цепной дроби представляет собой квадратичную иррациональность.*

Д о к а з а т е л ь с т в о. Пусть $\alpha = [q_0;\ q_1,\ q_2,\ \ldots]$ представляет собой бесконечную периодическую цепную дробь, т.е. существуют k и t $(t > 1)$ такие, что $\alpha_{k+t} = \alpha_k$. Согласно теореме 15 и замечанию к ней

$$\alpha_k = \frac{P_{k-2} - \alpha Q_{k-2}}{\alpha Q_{k-1} - P_{k-1}}, \quad \alpha_{k+t} = \frac{P_{k+t-2} - \alpha Q_{k+t-2}}{\alpha Q_{k+t-1} - P_{k+t-1}},$$

следовательно,

$$\frac{P_{k-2}-\alpha Q_{k-2}}{\alpha Q_{k-1}-P_{k-1}}=\frac{P_{k+t-2}-\alpha Q_{k+t-2}}{\alpha Q_{k+t-1}-P_{k+t-1}}.$$

Это равенство после приведения к общему знаменателю дает квадратное уравнение с целыми коэффициентами:

$$A\alpha^2+B\alpha+C=0,$$

где $A = Q_{k-1}Q_{k+t-2} - Q_{k-2}Q_{k+t-1}$. При $k = 0$ $A = Q_{-1}Q_{k-2} - Q_{-2}Q_{k-1} = -Q_{k-1} \neq 0$. Докажем от противного, что $A \neq 0$ и при $k \geqslant 1$.

Из соотношения (10) следует, что в последовательности

$$Q_{-1}=0,\ Q_0=1\leqslant Q_1<Q_2<\ldots \tag{25}$$

любые два соседних знаменателя взаимно просты. Если предположить, что $A = 0$ при некотором $k \geqslant 1$, то $\dfrac{Q_{k-2}}{Q_{k-1}} = \dfrac{Q_{k+t-2}}{Q_{k+t-1}}$. Из равенства этих двух несократимых дробей следует

$$Q_{k+t-2}=Q_{k-2},\quad Q_{k+t-1}=Q_{k-1},$$

а это противоречит тому, что при $k \geqslant 1$, $t \geqslant 1$ в последовательности (25) имеются самое большое два равных знаменателя.

Иррациональность числа α следует из того, что разложение α в цепную дробь бесконечно. Теорема доказана.

З а м е ч а н и е.

1. Квадратичная иррациональность $\alpha = \dfrac{P+\sqrt{D}}{Q}$, где P, Q и D $(D > 1)$ целые, разлагается в чисто периодическую цепную дробь тогда и только тогда, когда $\alpha > 1$ и

сопряженная иррациональность $\overline{\alpha} = \dfrac{P - \sqrt{D}}{Q}$ заключена в интервале $(-1;\ 0)$.

2. Если D — натуральное число, не являющееся точным квадратом, Q — целое, причем $D > Q^2 > 0$, то разложение $\dfrac{\sqrt{D}}{Q}$ в цепную дробь имеет вид:

$$\frac{\sqrt{D}}{Q} = [q_0;\ (q_1,\ q_2,\ \ldots,\ q_{t-1},\ 2q_0)]\,.$$

З а д а ч а 14. Разложить положительный корень квадратного уравнения $x^2 - 11 = 0$ в бесконечную периодическую цепную дробь.

Р е ш е н и е. Имеем: $\alpha = \sqrt{11}$. Тогда:

$$q_0 = \left[\sqrt{11}\right] = 3,$$

$$\alpha_1 = \frac{1}{\sqrt{11} - 3} = \frac{1 \cdot (\sqrt{11} + 3)}{(\sqrt{11} - 3)(\sqrt{11} + 3)} = \frac{\sqrt{11} + 3}{2},$$

$$q_1 = \left[\frac{\sqrt{11} + 3}{2}\right] = 3,$$

$$\alpha_2 = \frac{1}{\dfrac{\sqrt{11} + 3}{2} - 3} = \frac{2}{\sqrt{11} - 3} = \sqrt{11} + 3,$$

$$q_2 = \left[\sqrt{11} + 3\right] = 6,$$

$$\alpha_3 = \frac{1}{(\sqrt{11} + 3) - 6} = \frac{1}{\sqrt{11} - 3} = \frac{\sqrt{11} + 3}{2}.$$

Поскольку $\alpha_3 = \alpha_1$, будем иметь: $q_3 = [\alpha_3] = [\alpha_1] = q_1 = 3$, так что $\alpha_4 = \alpha_2$ и т.д. Таким образом,

$$\sqrt{11} = 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{6 + \ddots}}}} = [3;\ (3,\ 6)].$$

З а д а ч а 15. Найти квадратичную иррациональность, которая обращается в цепную дробь $[(1,\ 3)]$.

Р е ш е н и е. Имеем:

$$[(1,\ 3)] = 1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{3 + \ddots}}}.$$

Так как выражение, начинающееся с третьего полного частного, имеет тот же вид, что и исходное разложение, то можно записать: $\alpha = [1;\ 3,\ \alpha] = 1 + \cfrac{1}{3 + \cfrac{1}{\alpha}} = 1 + \cfrac{\alpha}{3\alpha + 1}$. После элементарных преобразований придем к квадратному уравнению относительно α: $3\alpha^2 - 3\alpha - 1 = 0$. Тогда, учитывая, что в нашем случае $\alpha > 0$, получим: $\alpha = \cfrac{3 + \sqrt{21}}{4}$.

Глава IV. Числовые сравнения

§1. Числовые сравнения и их свойства

1. Сравнение по модулю. Пусть дано кольцо целых чисел $\langle \mathbb{Z},\ +,\ \cdot \rangle$ и m — некоторое фиксированное натуральное число. Тогда, по теореме о делении с остатком, для всякого целого числа a существует единственная пара целых чисел q и r — таких, что $a = mq + r$, $0 \leqslant r < m$. Упомянутая теорема является основой следующего определения:

О п р е д е л е н и е 1. Если два целых числа a и b при делении на натуральное число m дают один и тот же остаток r, так что $a = mq_1 + r$ и $b = mq_2 + r$, $0 \leqslant r < m$, то они называются *равноостаточными*, или *сравнимыми по модулю* m. Это записывается следующим образом: $a \equiv b \pmod{m}$.

З а м е ч а н и е. Если $a \vdots m$, то $a \equiv 0 \pmod{m}$.

Т е о р е м а 1. (к р и т е р и й с р а в н и м о с т и). *Для того, чтобы целые числа a и b были сравнимы по модулю m, необходимо и достаточно, чтобы разность $(a - b)$ делилась на m.*

Д о к а з а т е л ь с т в о.

Н е о б х о д и м о с т ь. Если $a \equiv b \pmod{m}$, то по определению сравнения $(a = mq_1 + r)\ \ \&\ \ (b = mq_2 + r)$, где $0 \leqslant r < m$, $q_1,\ q_2$ — целые числа. Вычтем из первого равенства второе, тогда $a - b = m(q_1 - q_2)$, откуда $(a - b) \vdots m$.

Д о с т а т о ч н о с т ь. Пусть теперь имеем $(a - b) \vdots m$, следовательно, $\exists t \in \mathbb{Z} \mid (a - b) = mt$. Поделим b на m с остатком: $b = mq + r$, где $0 \leqslant r < m$. Тогда $a - (mq + r) = mt$ или $a = m(q + t) + r$, т.е. a при делении на m дает остаток r. Теорема доказана.

З а м е ч а н и е. Мы получили другое (эквивалентное) определение отношения сравнимости двух целых чисел a и b:

О п р е д е л е н и е 2. Два целых числа называются *сравнимыми по модулю* m, если их разность делится на m.

Итак, $a \equiv b \pmod m \Leftrightarrow (a-b) \vdots m \Leftrightarrow a = b + mt$, где $t \in \mathbb{Z}$.

П р и м е р ы.

1. $m = 3;\ 8 \equiv 5 \pmod 3$, так как $8 - 5 = 3$ и $3 \vdots 3$.
2. $m = 5;\ 12 \equiv 2 \pmod 5$, так как $12 - 2 = 10$ и $10 \vdots 5$.
3. $m = 2;\ 3 \equiv 7 \pmod 2$, так как $3 - 7 = -4$ и $-4 \vdots 2$.
4. $m = 5;\ 11 \not\equiv 3 \pmod 5$, так как $11 - 3 = 8$ и $8 \not\vdots 5$.

Т е о р е м а 2. *Отношение сравнимости по модулю* m *в кольце* $\langle \mathbb{Z},\ +,\ \cdot \rangle$ *является отношением эквивалентности.*

Д о к а з а т е л ь с т в о. Если $a \varphi b \overset{\text{df}}{\Leftrightarrow} a \equiv b \pmod m$, то очевидно выполнение следующих требований:

1. $\forall a \in \mathbb{Z},\ \forall m \in \mathbb{N}\ a \equiv a \pmod m$. Действительно, $(a - a) \vdots m$, т.е. φ — рефлексивно.

2. $\forall a,\ b \in \mathbb{Z}$, если $a \equiv b \pmod m$, то и $b \equiv a \pmod m$. В самом деле: $(a - b) \vdots m \Rightarrow a - b = mt,\ t \in \mathbb{Z} \Rightarrow b - a = m \cdot (-t),\ (-t) \in \mathbb{Z}$, т.е. φ — симметрично.

3. $\forall a,\ b,\ c \in \mathbb{Z}$, если $a \equiv b \pmod m$ и $b \equiv c \pmod m$, то $a \equiv c \pmod m$. Убедимся в этом: так как $[(a - b) \vdots m]\ \&\ [(b - c) \vdots m]$, то $\exists q_1,\ q_2 \in \mathbb{Z} \mid (a - b = mq_1)\ \&\ (b - c = mq_2)$. Сложив эти два равенства, будем иметь: $a - c = m(q_1 + q_2) \Rightarrow a \equiv c \pmod m$, т.е. φ — транзитивно. Теорема доказана.

2. Основные свойства числовых сравнений. Свойства сравнений во многом подобны свойствам числовых ра-

венств. Рассмотрим группу свойств, которые не зависят от модуля.

Свойство 1. *Сравнения по одному и тому же модулю можно почленно складывать.*

Доказательство. Пусть $a \equiv b \pmod m$ и $c \equiv d \pmod m$, тогда $\exists q_1,\ q_2 \in \mathbb{Z} \mid a-b=mq_1$ и $c-d=mq_2$. Сложим эти равенства: $(a-b)+(c-d)=m(q_1+q_2) \Rightarrow$ $\Rightarrow (a+c)-(b+d)=m(q_1+q_2) \Rightarrow a+c \equiv b+d \pmod m$. Свойство доказано.

Свойство 2. *Сравнения по одному и тому же модулю можно почленно вычитать одно из другого.*

Доказательство. Пусть $a \equiv b \pmod m$ и $c \equiv d \pmod m$, тогда $\exists q_1,\ q_2 \in \mathbb{Z} \mid a-b=mq_1$ и $c-d=mq_2$. Вычтем второе равенство из первого: $(a-c)-(b-d)=$ $=m(q_1-q_2)$, следовательно, $a-c \equiv b-d \pmod m$. Свойство доказано.

Следствие. *Если $a \equiv b \pmod m$ и $k \in \mathbb{Z}$, то $a+k \equiv b+k \pmod m$ и $a-k \equiv b-k \pmod m$.*

Доказательство. Так как отношение сравнимости в кольце целых чисел рефлексивно (см. теорему 2), имеем: $k \equiv k \pmod m$. Согласно свойствам 1 и 2, складывая сравнения $a \equiv b \pmod m$ и $k \equiv k \pmod m$ почленно, получим: $a+k \equiv b+k \pmod m$, а вычитая из сравнения $a \equiv b \pmod m$ сравнение $k \equiv k \pmod m$ почленно, будем иметь $a-k \equiv b-k \pmod m$. Следствие доказано.

Следствие. *Члены сравнения можно переносить из одной части сравнения в другую с противоположным знаком.*

Доказательство. Ввиду симметричности отношения сравнимости (теорема 2) достаточно рассмотреть

случай, когда дано сравнение $a + b \equiv c \pmod{m}$. Действительно, из $a + b \equiv c \pmod{m}$ следует $a \equiv c - b \pmod{m}$, если данное сравнение сложить со вспомогательным сравнением $-b \equiv -b \pmod{m}$. Следствие доказано.

С л е д с т в и е. *К любой части сравнения можно прибавить целое число, кратное модулю.*

Д о к а з а т е л ь с т в о. Так как отношение сравнимости симметрично (теорема 2), то можно рассмотреть только один случай, когда из $a \equiv b \pmod{m}$ следует $a + mk \equiv \equiv b \pmod{m}$, если взять вспомогательное сравнение $mk \equiv 0 \pmod{m}$, $k \in \mathbb{Z}$ и сложить его с исходным. Следствие доказано.

С в о й с т в о 3. *Сравнения по одному и тому же модулю можно почленно перемножать.*

Д о к а з а т е л ь с т в о. Пусть $a \equiv b \pmod{m}$ и $c \equiv \equiv d \pmod{m}$, тогда $a = b + mq_1$ и $c = d + mq_2$, q_1, $q_2 \in \mathbb{Z}$. Перемножим последние равенства: $ac = bd + bmq_2 + dmq_1 + +m^2q_1q_2$, или же $ac = bd + m(bq_2 + dq_1 + mq_1q_2) \Rightarrow ac \equiv \equiv bd \pmod{m}$. Свойство доказано.

С л е д с т в и е. *Обе части сравнения можно возводить в одну и ту же неотрицательную степень: если $a \equiv b \pmod{m}$ и k — целое неотрицательное число, то $a^k \equiv b^k \pmod{m}$.*

Д о к а з а т е л ь с т в о. Действительно, из сравнения $a \equiv b \pmod{m}$ следует $a^k \equiv b^k \pmod{m}$, которое получается при почленном перемножении k сравнений, каждое из которых равно данному. Следствие доказано.

С в о й с т в о 4. *Обе части сравнения можно умножать на одно и то же целое число.*

Д о к а з а т е л ь с т в о. Перемножив почленно сравне-

ние $a \equiv b \pmod m$ с очевидным сравнением $k \equiv k \pmod m$, получим: $ak \equiv bk \pmod m$. Свойство доказано.

Приведем теперь свойства сравнений, зависящие от модуля.

Свойство 5. *Если* $a \equiv b \pmod m$ *и* $m \vdots n$, *то* $a \equiv b \pmod n$.

Доказательство. Так как $a \equiv b \pmod m$, то $(a-b) \vdots m$. А так как $m \vdots n$, то в силу транзитивности отношения делимости $(a-b) \vdots n$, значит $a \equiv b \pmod m$. Свойство доказано.

Свойство 6. *Обе части сравнения и модуль можно умножать на одно и то же натуральное число.*

Доказательство. Пусть $a \equiv b \pmod m$ и $k \in \mathbb{N}$. Тогда $a - b = mq$, $q \in \mathbb{Z}$ и $ak - bk = mqk$, или $ak \equiv bk \pmod{mk}$. Свойство доказано.

Свойство 7. *Если* $ak \equiv bk \pmod m$ *и* $(k,\ m) = d$, *то* $a \equiv b \left(\mathrm{mod}\ \dfrac{m}{d}\right)$.

Доказательство. Пусть $k = k_1 d$, а $m = m_1 d$. Из $ak = bk \pmod m$ следует $(ak - bk) \vdots m$ или $(a-b) \cdot k_1 d \vdots m_1 d$, откуда $(a-b)k_1 \vdots m_1$. Так как $(k_1,\ m_1) = 1$, то, (см. «Предварительные сведения», утверждение 3), $(a-b) \vdots m_1$, или $(a-b) \vdots \dfrac{m}{d}$, т.е. $a \equiv b \left(\mathrm{mod}\ \dfrac{m}{d}\right)$. Свойство доказано.

Замечание.

1. Если в свойстве 7 положить $d = k$, т.е. если $m \vdots k$ (докажите самостоятельно эквивалентность этих условий, используя основные факты теории делимости в кольце целых чисел), то из $ak \equiv bk \pmod m$ следует $a \equiv b \left(\mathrm{mod}\ \dfrac{m}{k}\right)$,

а это означает, что обе части сравнения и модуль можно разделить на их общий делитель.

2. Если в свойстве 7 положить $d = 1$, т.е. если $(k,\ m) = 1$, то из $ak \equiv bk \pmod{m}$ следует $a \equiv b \pmod{m}$, а это значит, что обе части сравнения можно разделить на их общий делитель, если он взаимно прост с модулем.

Свойство 8. *Общий делитель одной части сравнения и модуля является также делителем второй части.*

Доказательство. Так как отношение сравнимости симметрично (теорема 2), то рассмотрим один случай, когда d — общий делитель чисел a и m. Имеем: $a = a_1 \cdot d$ и $m = m_1 \cdot d$, где $a_1,\ m_1 \in \mathbb{Z}$. Из $a \equiv b \pmod{m}$ следует $a = b + mt,\ t \in \mathbb{Z}$ или $a_1 d - m_1 dt = b \Rightarrow b \vdots d$. Свойство доказано.

Доказанное свойство показывает, что все делители пар чисел a и m, а также b и m являются общими. Это относится и к их наибольшим общим делителям. Таким образом, мы приходим к важному следствию.

Следствие. *Части сравнения и модуль имеют одинаковый наибольший общий делитель, т.е.* $(a,\ m) = (b,\ m)$.

В частности, если $(a,\ m) = 1$, то и $(b,\ m) = 1$. Другими словами, если одна часть сравнения и модуль числа взаимно простые, то и вторая часть сравнения и модуль числа взаимно простые.

Из рассмотренных свойств сравнений вытекает следующее общее свойство:

Свойство 9. *Пусть* $P(x)$ — *многочлен с целыми коэффициентами,* a *и* b — *целые числа. Тогда, если* $a \equiv b \pmod{m}$, *то* $P(a) \equiv P(b) \pmod{m}$.

Д о к а з а т е л ь с т в о. Пусть

$$P(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0.$$

По условию $a \equiv b \pmod m$, тогда $a^k \equiv b^k \pmod m$ при $k = 0, 1, 2, \ldots, n$. Почленно умножая обе части каждого из полученных $n + 1$ сравнений на сравнение $c_k \equiv \equiv c_k \pmod m$, получим:

$$c_k a^k \equiv c_k b^k \pmod m,$$

где $k = 0, 1, 2, \ldots, n$. Складывая последние сравнения, получим:

$$P(a) \equiv P(b) \pmod m.$$

Свойство доказано.

С л е д с т в и е. Если при $a \equiv b \pmod m$ еще и $c_k \equiv \equiv d_k \pmod m$, то

$$c_n a^n + c_{n-1} a^{n-1} + \ldots + c_1 a + c_0 \equiv$$

$$\equiv d_n b^n + d_{n-1} b^{n-1} + \ldots + d_1 b + d_0 \pmod m.$$

Д о к а з а т е л ь с т в о. Чтобы убедиться в справедливости этого следствия, достаточно в доказательстве свойства 9 почленно умножить каждое сравнение $a^k \equiv \equiv b^k \pmod m$, $k = 0, 1, 2, \ldots, n$ на сравнение $c_k \equiv \equiv d_k \pmod m$ и далее провести аналогичные рассуждения. Следствие доказано.

Таким образом, в сравнении

$$c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0 \equiv 0 \pmod m$$

слагаемые и множители можно заменять числами, сравнимыми по тому же модулю m. Например, сравнения

$$6x^5 + 4x^4 + 10x^3 + 12x^2 - 5 \equiv 0 \pmod 4$$

и

$$2x^5 + 2x^3 - 1 \equiv 0 \pmod 4$$

эквивалентны.

Свойство 9 имеет ряд важный применений. В частности, с его помощью можно дать теоретическое обоснование признаков делимости, которое будет установлено нами в §4 этой главы.

§2. Классы вычетов по данному модулю

1. Кольцо классов вычетов по модулю m. Так как отношение сравнимости целых чисел является отношением эквивалентности (теорема 2), то все множество целых чисел можно разбить на непересекающиеся классы сравнимых между собой по модулю m целых чисел. Приходим к определению.

О п р е д е л е н и е 3. Пусть a — произвольное целое число. Множество всех чисел, сравнимых с a по модулю m, называется *классом вычетов по модулю* m (с *представителем* a) и обозначается символом $\overline{a}$. Любое число из класса $\overline{a}$ называется *вычетом* числа a по модулю m.

Т е о р е м а 3. *Для того, чтобы два класса с представителями* a *и* b *совпадали, необходимо и достаточно, чтобы* $a \equiv b \pmod m$.

Д о к а з а т е л ь с т в о.

Н е о б х о д и м о с т ь. Если $\overline{a} = \overline{b}$, то это означает, что $a \in \overline{b}$, $a \equiv b \pmod m$.

Д о с т а т о ч н о с т ь. Если $a \equiv b \pmod m$, то $\forall x \in \overline{a}\ x \equiv a \pmod m$; пользуясь транзитивностью отношения сравнимости, получаем $x \equiv b \pmod m \Rightarrow x \in \overline{b}$. В

силу симметричности отношения сравнимости (теорема 2), $\forall x \in \overline{b} \Rightarrow x \in \overline{a}$. Классы $\overline{a}$ и $\overline{b}$, таким образом, совпадают. Теорема доказана.

З а м е ч а н и е. Эта теорема позволяет, таким образом, заменять сравнение равенством соответствующих классов и, наоборот, равенство классов — соответствующим сравнением.

Т е о р е м а 4. *Если два класса имеют хотя бы один общий элемент, то они совпадают.*

Д о к а з а т е л ь с т в о. Пусть $\left(x \in \overline{a}\right)$ & $\left(x \in \overline{b}\right)$, тогда $[x \equiv a \pmod m]$ & $[x \equiv b \pmod m]$. Но так как отношение сравнимости симметрично и транзитивно (теорема 2), то $x \equiv b \pmod m$) и по предыдущей теореме $\overline{a} = \overline{b}$. Теорема доказана.

З а м е ч а н и е. Из этой теоремы следует, что два класса вычетов по модулю m либо не имеют общих элементов, либо полностью совпадают.

Т е о р е м а 5. *Количество классов вычетов по модулю m конечно и равно m. При этом в качестве представителей классов можно брать числа* $0,\ 1,\ 2,\ \ldots,\ m-1$.

Д о к а з а т е л ь с т в о. Из теоремы о делении с остатком следует, что каждое число сравнимо по модулю m со своим остатком при делении на m (докажите это самостоятельно!). И поскольку таких остатков существует ровно m (это $0,\ 1,\ 2,\ \ldots,\ m-1$), то множество классов вычетов по модулю m не может содержать больше, чем m классов.

С другой стороны, числа $0,\ 1,\ 2,\ \ldots,\ m-1$ принадлежат разным классам вычетов по модулю m. Действительно, взяв числа a и b из множества $\left\{0,\ 1,\ 2,\ \ldots,\ m-1\right\}$, видим, что $(a-b) \not\vdots m$, т.е. $a \not\equiv b \pmod m$. Таким образом, суще-

ствует не менее m различных классов вычетов по модулю m: $\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{m-1}$. Теорема доказана.

Т е о р е м а 6. *Числа класса $\overline{a}$ по модулю k образуют k классов по модулю km, а именно классы:*

$$\overline{a},\ \overline{a+m},\ \overline{a+2m},\ \ldots,\ \overline{a+(k-1)m}. \tag{26}$$

Д о к а з а т е л ь с т в о. Возьмем некоторый класс $\overline{a}$. Для любого представителя x этого класса будет $x \equiv a \pmod m \Rightarrow (x-a) \vdots m \Rightarrow x-a=mt,\ t \in \mathbb{Z} \Rightarrow x = a+mt$, поэтому все числа класса $\overline{a}$ имеют вид: $a+mt$, $t \in \mathbb{Z}$, т.е.

$$\ldots,\ a-2m,\ a-m,\ a,\ a+m,\ a+2m,\ \ldots \tag{27}$$

Докажем, что находящиеся среди них числа

$$a,\ a+m,\ a+2m,\ \ldots,\ a+(k-1)m \tag{28}$$

попарно несравнимы по модулю km, т.е. лежат в разных классах по этому модулю. Действительно, абсолютная величина разности между двумя любыми числами из последовательности (28) будет положительной и вместе с тем не больше, чем разность между самым большим из них $a+(k-1)m$ и самым маленьким a, т.е. не больше, чем $(k-1)m$. Такая разность не может делиться на km, а следовательно, среди этих чисел нет сравнимых по модулю km.

Таким образом, классы

$$\overline{a},\ \overline{a+m},\ \overline{a+2m},\ \ldots,\ \overline{a+(k-1)m}$$

по модулю km различны, причем ясно, что все числа каждого такого класса целиком входят в множество (27). Докажем теперь, что любое число из (27) сравнимо с одним из

чисел (28). Любое число из (27) имеет вид $a + mt$, $t \in \mathbb{Z}$. Представим t в виде $t = kq + r$ $(0 \leqslant r < k)$. Тогда

$$a+mt = a+m(kq+r) = a+rm+kmq \equiv a+rm \pmod{km},$$

где $a + rm$ — одно из чисел множества (28). Таким образом, все числа класса вычетов $\overline{a}$ по модулю m принадлежат к различным по модулю km классам (26), не содержащим каких-либо чисел, отличных от чисел вида (27). Теорема доказана.

Понятно, что множество классов вычетов по модулю m есть фактор-множество $\mathbb{Z}/\varphi$ множества целых чисел $\mathbb{Z}$ по отношению эквивалентности $\varphi \stackrel{\text{df}}{=} a \equiv b \pmod{m}$. Обозначим это фактор-множество через $\mathbb{Z}_m$ и определим на этом нем две бинарные операции сложения и умножения классов. Чтобы сложить классы вычетов $\overline{k}$ и $\overline{s}$ по модулю m, надо выбрать в $\overline{k}$ число k, в $\overline{s}$ число s, сложить эти числа и взять класс вычетов, содержащий $k + s$; этот класс вычетов и является суммой $\overline{k}$ и $\overline{s}$. Точно также определяется умножение классов вычетов.

Иными словами,

$$\overline{k} \oplus \overline{s} = \overline{k+s}, \quad \overline{k} \odot \overline{s} = \overline{k \cdot s}.$$

Поскольку каждый класс содержит бесконечное множество чисел, то при сложении и умножении классов $\overline{a}$ и $\overline{b}$ числа a и b можно заменять любыми числами a' и b', принадлежащими этим же классам. Возникает вопрос, меняются ли при этом определенные нами сумма и произведение классов. Легко доказать, что сумма и произведение классов определяются единственным образом и не зависят от выбора отдельных представителей классов.

Действительно, если $a' \in \overline{a}$ и $b' \in \overline{b}$, то $a' \equiv a \pmod m$ и $b' \equiv b \pmod m$. Применяя свойства 1 и 3 сравнений, получаем:

$$a' + b' \equiv a + b \pmod m, \quad a'b' \equiv ab \pmod m,$$

т.е. (теорема 3)

$$\overline{a' + b'} = \overline{a + b}, \quad \overline{a'b'} = \overline{ab}.$$

Мы видим, таким образом, что сумма и произведение классов не меняются от замены a и b числами a' и b'. Сумма классов $\overline{a}$ и $\overline{b}$ содержит сумму любого числа $a' \in \overline{a}$ и $b' \in \overline{b}$, а произведение классов $\overline{a}$ и $\overline{b}$ содержит произведение любых таких чисел a' и b'.

Т е о р е м а 7. *Алгебра* $\langle \mathbb{Z}_m, \oplus, \odot \rangle$ *является коммутативно-ассоциативным кольцом с единицей.*

Д о к а з а т е л ь с т в о. Докажем сначала, что $\langle \mathbb{Z}_m, \oplus \rangle$ — абелева группа.

а) Замкнутость множества $\mathbb{Z}_m$ относительно операций сложения и умножения классов вычетов следует из определения этих операций:

$$\forall \overline{k}, \ \overline{s} \in \mathbb{Z}_m \ \left[\left(\overline{k} \oplus \overline{s}\right) \in \mathbb{Z}_m\right] \ \& \ \left[\left(\overline{k} \odot \overline{s}\right) \in \mathbb{Z}_m\right].$$

б) Операции сложения классов вычетов ассоциативна:

$$\forall \overline{k}, \ \overline{s}, \ \overline{r} \in \mathbb{Z}_m \ \left(\overline{k} \oplus \overline{s}\right) \oplus \overline{r} = \overline{k} \oplus \left(\overline{s} \oplus \overline{r}\right),$$

так как

$$\left(\overline{k} \oplus \overline{s}\right) \oplus \overline{r} = \overline{k + s} \oplus \overline{r} = \overline{k + s + r}$$

и

$$\overline{k} \oplus \left(\overline{s} \oplus \overline{r}\right) = \overline{k} \oplus \overline{s + r} = \overline{k + s + r}.$$

в) В множестве $\mathbb{Z}_m$ роль нейтрального элемента по сложению играет $\overline{0}$:

$$\exists\overline{0} \in \mathbb{Z}_m \mid \forall\overline{k} \in \mathbb{Z}_m\ \overline{0} \oplus \overline{k} = \overline{k} \oplus \overline{0} = \overline{k}.$$

Эту и следующие аксиомы проверьте самостоятельно!

г) В множестве $\mathbb{Z}_m$ каждый класс вычетов имеет себе противоположный:

$$\forall\overline{k} \in \mathbb{Z}_m\ \exists\overline{(-k)} \in \mathbb{Z}_m \mid \overline{k} \oplus \overline{(-k)} = \overline{(-k)} \oplus \overline{k} = \overline{0}.$$

д) Операция сложения классов вычетов коммутативна:

$$\forall\overline{k},\ \overline{s} \in \mathbb{Z}_m\ \overline{k} \oplus \overline{s} = \overline{s} \oplus \overline{k}.$$

Итак, $\langle \mathbb{Z}_m,\ \oplus \rangle$ — абелева группа.

е) Операции сложения и умножения классов вычетов на множестве $\mathbb{Z}_m$ связаны левым и правым дистрибутивными законами:

$$\forall\overline{k},\ \overline{s},\ \overline{r} \in \mathbb{Z}_m\ \overline{k} \odot \left(\overline{s} \oplus \overline{r}\right) = \overline{k} \odot \overline{s} \oplus \overline{k} \odot \overline{r}$$

и

$$\left(\overline{s} \oplus \overline{r}\right) \odot \overline{k} = \overline{s} \odot \overline{k} \oplus \overline{r} \odot \overline{k}.$$

ж) Операция умножения классов вычетов коммутативна:

$$\forall\overline{k},\ \overline{s} \in \mathbb{Z}_m\ \overline{k} \odot \overline{s} = \overline{s} \odot \overline{k}.$$

з) Операции умножения классов вычетов ассоциативна:

$$\forall\overline{k},\ \overline{s},\ \overline{r} \in \mathbb{Z}_m\ \left(\overline{k} \odot \overline{s}\right) \odot \overline{r} = \overline{k} \odot \left(\overline{s} \odot \overline{r}\right).$$

и) Класс вычетов $\overline{1}$ является нейтральным элементом относительно операции умножения классов:

$$\exists\overline{1} \in \mathbb{Z}_m \mid \forall\overline{k} \in \mathbb{Z}_m\ \overline{1} \odot \overline{k} = \overline{k} \odot \overline{1} = \overline{k}.$$

Итак, $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ — коммутативно-ассоциативное кольцо с единицей. Это кольцо и называют *кольцом классов вычетов по модулю* m. Теорема доказана.

З а м е ч а н и е. Аддитивная абелева группа $\mathbb{Z}_m$ кольца $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ состоит из m элементов: $\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{m-1}$, кратных классу вычетов $\overline{1}$, поэтому она является циклической группой порядка m, порожденной $\overline{1}$.

Поскольку подкольцо $m\mathbb{Z}$ — главный идеал (порожденный элементом m) в кольце $\mathbb{Z}$, то $\mathbb{Z}_m$ является факторкольцом кольца $\mathbb{Z}$ по идеалу $m\mathbb{Z} = (m)$, т.е. $\mathbb{Z}_m = \mathbb{Z}/(m)$ (см. «Алгебра», часть 3).

Так как кольцо $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ конечно, то операции в нем можно задавать конечными таблицами сложения и умножения.

П р и м е р. Напишем таблицы сложения и умножения для кольца $\langle \mathbb{Z}_6,\ \oplus,\ \odot \rangle$. Здесь мы имеем 6 классов вычетов: $\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}$. Таблицы сложения и умножения имеют вид:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2. Полная и приведенная системы вычетов, их свойства. Пусть дано множество классов вычетов

$$\mathbb{Z}_m = \{\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{m-1}\}.$$

Выберем из каждого класса по одному вычету (представителю этого класса). Получим m целых чисел: $x_0,\ x_1,\ x_2,\ \ldots,\ x_{m-1}$.

О п р е д е л е н и е 4. Множество $\{x_0,\ x_1,\ x_2,\ \ldots,\ x_{m-1}\}$ называется *полной системой вычетов по модулю m.*

Так как классы вычетов являются бесконечными множествами, то можно составить бесконечного много различных полных систем вычетов по данному модулю m, каждая из которых содержит m вычетов.

П р и м е р. Составим несколько полных систем вычетов по модулю 5. Здесь имеем 5 классов вычетов:

$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
...	...	...	...	...
-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
...	...	...	...	...

Любая полная система вычетов по модулю 5 будет содержать 5 чисел, взятых по одному разу из каждого класса. Выпишем несколько таких систем:

$$\begin{array}{rrrrr} 0, & 1, & 2, & 3, & 4 \\ 10, & 6, & 2, & 8, & 9 \\ -10, & -9, & -8, & -7, & -6 \\ -5, & 1, & -3, & -7, & -1 \end{array}$$

и т.д.

О п р е д е л е н и е 5. Вычет класса $\overline{a}$, равный остатку от деления числа a на модуль m, называется *наименьшим неотрицательным вычетом.*

О п р е д е л е н и е 6. Вычет, наименьший по абсолютной величине, называется *абсолютно наименьшим вычетом.*

Наиболее употребительны следующие системы вычетов:

а) *Полная система наименьших неотрицательных вычетов:* $\overline{0}$, $\overline{1}$, $\overline{2}$, $\ldots$, $\overline{m-1}$. В приведенном выше примере: 0, 1, 2, 3, 4. Такая система составляется просто: надо выписать все остатки, получающиеся при делении на m.

б) *Полная система наименьших положительных вычетов:* 1, 2, $\ldots$, m. В нашем примере: 1, 2, 3, 4, 5.

в) *Полная система абсолютно наименьших вычетов.* В приведенном примере: -2, -1, 0, 1, 2. Если в классе содержится два вычета, a и $-a$, имеющие одинаковую абсолютную величину, то можно взять любой из них. Так, если $m = 8$, то из класса $\overline{4}$ можно взять вычет 4 или -4.

Т е о р е м а 8. *Все числа полной системы вычетов попарно несравнимы по модулю m.*

Д о к а з а т е л ь с т в о. Поскольку в полной системе вычетов из каждого класса взят ровно один представитель, то никакие два из них не могут быть сравнимы по модулю m, так как содержатся в разных классах вычетов. Теорема доказана.

Т е о р е м а 9 (п р и з н а к п о л н о й с и с т е м ы в ы ч е т о в). *Любая совокупность из m чисел, попарно несравнимых по модулю m, образует полную систему вычетов по модулю m.*

Д о к а з а т е л ь с т в о. По условию данные числа

несравнимы между собой по модулю m, поэтому они принадлежат разным классам вычетов по модулю m. При этом данных чисел всего m, т.е. столько же, сколько всего классов вычетов по модулю m. Следовательно, от каждого класса имеется по одному представителю, что и требуется для полной системы вычетов. Теорема доказана.

Т е о р е м а 10. *Если* $(a,\ m) = 1$, b — *произвольное целое число и* x *пробегает полную систему вычетов по модулю* m, *то и значения линейной формы* $ax + b$ *тоже пробегают полную систему вычетов по модулю* m.

Д о к а з а т е л ь с т в о. Чисел $ax+b$ столько же, сколько и чисел x, т.е. m. По установленному признаку полной системы вычетов остается доказать, что любые два числа $ax_1 + b$ и $ax_2 + b$, соответствующие несравнимым x_1 и x_2, сами несравнимы по модулю m. Докажем это методом от противного. Допустим, что $ax_1 + b \equiv ax_2 + b \pmod{m}$. Вычтем из обеих частей этого сравнения по b и разделим обе части полученного сравнения на a, взаимно простое с модулем по условию. Тогда $x_1 \equiv x_2 \pmod{m}$, что противоречит условию теоремы 8 (x пробегает полную систему вычетов по модулю m). Теорема доказана.

Т е о р е м а 11. *Для того, чтобы кольцо вычетов* $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ *было полем, необходимо и достаточно, чтобы модуль* m *был простым числом. Если* m — *составное число, то в кольце* $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ *есть делители нуля.*

Д о к а з а т е л ь с т в о.

Н е о б х о д и м о с т ь. Пусть $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ — поле. Нужно доказать, что m — простое число. Предположим противное: пусть $m = 1$ или же m — составное число. В случае, когда $m = 1$, очевидно, что $\mathbb{Z}_m = \mathbb{Z}$, а $\mathbb{Z}$ — не является

полем (см. «Алгебра», часть 1). Имеем противоречие с тем, что $\mathbb{Z}_m$ — поле.

Если m — составное число, то оно имеет делители k и l, каждый из которых по модулю меньше, чем m, $m = rs$, $|r| < m$, $|s| < m$. Но тогда классы вычетов $\overline{r}$ и $\overline{s}$ не являются нулевыми, в то время, как $\overline{r} \odot \overline{s} = \overline{r \cdot s} = \overline{m} = \overline{0}$. Значит, в $\mathbb{Z}_m$ есть делители нуля, а потому $\mathbb{Z}_m$ не является полем. Снова имеем противоречие с условием. Полученные противоречия указывают на неверность нашего предположения и доказывают необходимость.

Достаточность. Пусть m — простое число. Покажем, что тогда алгебра $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ является полем.

Нами уже доказано, что $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ — коммутативно-ассоциативное кольцо с единицей (см. теорему 7). Остается доказать, что любой ненулевой класс из $\mathbb{Z}_m$ будет симметризуем по умножению, т.е.

$$\forall \overline{r} \in \mathbb{Z}_m\ (\overline{r} \neq \overline{0})\ \exists \overline{x} \in \mathbb{Z}_m \mid \overline{r} \odot \overline{x} = \overline{x} \odot \overline{r} = \overline{1}.$$

Так как m — простое число, то $(r,\ m) = 1$ или $r \vdots m$ (см. «Алгебра», часть 1). Но число r не кратно m, ибо в противном случае при делении на m давало бы в остатке 0, и имели бы $\overline{r} = \overline{0}$. Таким образом, $(r,\ m) = 1$, и поэтому $\exists x,\ y \in \mathbb{Z} \mid rx + my = 1$. Отсюда вытекает, что $rx - 1 \vdots m$, т.е. $rx \equiv 1 \pmod{m}$. Но тогда $\overline{rx} = \overline{1}$ или $\overline{r} \odot \overline{x} = \overline{1}$, а так как операция умножения классов коммутативна, то и $\overline{x} \odot \overline{r} = \overline{1}$. Видим, что в кольце $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ существует класс $\overline{x}$, обратный к классу $\overline{r}$. Теорема доказана.

По следствию свойства 8 сравнений, сравнимые по модулю m числа, т.е. вычеты одного и того же класса по данному модулю имеют с этим модулем один и тот же наибольший общий делитель. Следовательно, если один вычет класса

взаимно прост с модулем, то и любой вычет этого класса тоже взаимно прост с модулем.

О п р е д е л е н и е 7. Наибольший общий делитель модуля m и любого числа a из данного класса вычетов по модулю m называется *наибольшим общим делителем* m и этого класса вычетов.

О п р е д е л е н и е 8. Класс вычетов $\overline{a}$ по модулю m называется *взаимно простым с модулем* m, если наибольший общий делитель класса $\overline{a}$ и m равен 1 (т.е. если m и любое число из $\overline{a}$ взаимно просты).

П р и м е р. Пусть $m = 8$. Класс $\overline{3}$ состоит из чисел $\{\ldots, -5, 3, 11, 19, \ldots\}$. Наибольший общий делитель любого из этих чисел и модуля 8 равен 1. Значит, $\left(\overline{3},\ 8\right) = 1$.

Выберем из каждого класса вычетов, взаимно простого с модулем m, по одному числу. Получим систему вычетов, составляющую часть полной системы вычетов.

О п р е д е л е н и е 9. Совокупность вычетов по модулю m, взятых по одному из каждого взаимно простого с модулем m класса вычетов по этому модулю, называется *приведенной системой вычетов по модулю* m.

Из определения следует способ получения приведенной системы вычетов по модулю m: надо выписать какую-либо полную систему вычетов и удалить из нее все вычеты, не взаимно простые с m. Оставшаяся совокупность вычетов — приведенная система вычетов по модулю m; понятно, что их можно составить бесчисленное множество. Если в качестве исходной взять полную систему наименьших неотрицательных или абсолютно наименьших вычетов, то указанным способом получим соответственно приведенную систему наименьших неотрицательных или абсолютно наимень-

ших вычетов по модулю m.

Пример. Так, если $m = 10$, то 1, 3, 7, 9 — приведенная система наименьших неотрицательных вычетов, 1, 3, -3, -1 — приведенная система абсолютно наименьших вычетов.

Теорема 12 (признак приведенной системы вычетов). *Пусть число классов, взаимно простых с m, равно k. Тогда любая совокупность из k целых чисел, попарно несравнимых по модулю m и взаимно простых с модулем m, образует приведенную систему вычетов по модулю m.*

Доказательство. По условию данные числа взаимно просты с модулем и попарно несравнимы по модулю m, поэтому они принадлежат разным классам, взаимно простым с модулем m. При этом данных чисел всего k, т.е. столько же, сколько всего классов, взаимно простых с модулем m. Следовательно, от каждого класса, взаимно простого с модулем, имеется по одному представителю, что и требуется для приведенной системы вычетов. Теорема доказана.

Теорема 13. *Если $(a, m) = 1$ и x пробегает приведенную систему вычетов по модулю m, то и значения линейной формы ax пробегают приведенную систему вычетов по модулю m.*

Доказательство. Пусть $x_1, x_2, \ldots, x_k$ — приведенная система вычетов по модулю m. Тогда в системе $ax_1, ax_2, \ldots, ax_k$ содержится ровно k чисел. Эти числа принадлежат различным классам по модулю m, т.е. они попарно несравнимы по модулю m, что было доказано в теореме 9. Наконец, каждое из чисел $ax_1, ax_2, \ldots, ax_k$ вза-

имно просто с модулем m, так как сомножители в отдельности взаимно просты с m (в силу утверждения 4 из раздела «Предварительные сведения»): $(a,\ m) = 1$ по условию теоремы, $(x_i,\ m) = 1,\ i = 1,\ 2,\ \ldots,\ k$, так как x_i — вычет приведенной системы. Таким образом, согласно установленному признаку приведенной системы (предыдущая теорема), числа $ax_1,\ ax_2,\ \ldots,\ ax_k$ образуют приведенную систему вычетов по модулю m.

З а м е ч а н и е. Надо иметь в виду, что соответственные отдельные значения x и ax в общем случае принадлежат различным классам. Например, пусть $a = 7,\ m = 12$ и x пробегает приведенную систему наименьших положительных вычетов по модулю 12: $1,\ 5,\ 7,\ 11$. Тогда ax пробегает значения $7,\ 35,\ 49,\ 77$, принадлежащие классам, наименьшие положительные вычеты в которых принимают значения $7,\ 11,\ 1,\ 5$ соответственно, т.е. те же значения, но расположенные по-иному.

Вопрос о количестве вычетов в приведенной системе по модулю m решается с помощью функции Эйлера, которой посвящен следующий параграф.

§3. Функция Эйлера. Теоремы Эйлера и Ферма

1. Функция Эйлера. Обозначим через $\varphi(m)$ число классов вычетов по модулю m, взаимно простых с m, т.е. число элементов приведенной системы вычетов по модулю m. Функция $\varphi(m)$ является числовой. Ее называют *функцией Эйлера.*

Выберем в качестве представителей классов вычетов по модулю m числа $1,\ 2,\ \ldots,\ m-1,\ m$. Тогда $\varphi(m)$ — количество таких чисел, которые взаимно просты с m. Другими

словами, $\varphi(m)$ — *количество натуральных чисел, не превосходящих* m *и взаимно простых с* m.

Примеры.

1. Пусть $m = 9$. Полная система вычетов по модулю 9 состоит из чисел 1, 2, 3, 4, 5, 6, 7, 8, 9. Из них взаимно просты с 9 числа 1, 2, 4, 5, 7, 8. Так как количество этих чисел равно 6, то $\varphi(9) = 6$.

2. Пусть $m = 12$. Здесь полная система вычетов состоит из чисел 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. Из них взаимно просты с 12 числа 1, 5, 7, 11. Значит, $\varphi(12) = 4$.

При $m = 1$ полная система вычетов состоит из одного класса $\overline{0} = \mathbb{Z}$. Наибольшим общим делителем любого целого числа и 1 является 1, т.е. $\left(\overline{0},\ 1\right) = 1$. На этом основании полагают $\varphi(1) = 1$.

Перейдем к вычислению функции Эйлера, но сначала докажем одно важное ее свойство.

Теорема 14. *Функция Эйлера мультипликативна, т.е.*

$$\forall m,\ n \in \mathbb{Z} \mid (m,\ n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Доказательство. Чтобы найти $\varphi(m \cdot n)$, нужно узнать количество натуральных чисел ряда $1,\ 2,\ \ldots,\ m \cdot n$, взаимно простых с $m \cdot n$. Расположим числа этого ряда в виде следующей таблицы:

1	2	3	$\ldots$	k	$\ldots$	n
$n+1$	$n+2$	$n+3$	$\ldots$	$n+k$	$\ldots$	$2n$
$2n+1$	$2n+2$	$2n+3$	$\ldots$	$2n+k$	$\ldots$	$3n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$(m-1)n+1$	$(m-1)n+2$	$(m-1)n+3$	$\ldots$	$(m-1)n+k$	$\ldots$	mn

Известно, что взаимно простыми с mn являются те и только те числа, которые взаимно просты как с m, так и

с n (см. «Предварительные сведения», утверждение 4). Поэтому отберем из этой таблицы сначала все числа, взаимно простые с n, а затем те из них, которые взаимно просты с m.

Числа одного столбца принадлежат одному классу вычетов по модулю n, поэтому все они имеют с n одинаковый наибольший общий делитель. Если одно из этих чисел взаимно просто с n, то и остальные числа этого столбца взаимно просты с n.

Найдем число столбцов, элементы которых взаимно просты с n. О нем можно судить по количеству чисел одной строки, например первой, взаимно простых с n. Очевидно поэтому, что число столбцов, состоящих из элементов, взаимно простых с n, равно $\varphi(n)$.

Теперь остается выделить из этих $\varphi(n)$ столбцов те числа, которые взаимно просты с m. Рассмотрим теперь любой столбец таблицы, например k-ый:

$$k,\ n+k,\ 2n+k,\ \ldots,\ (m-1)n+k.$$

Числа этого столбца можно рассматривать как значения линейной формы $nx + k$, когда x пробегает значения $0,\ 1,\ \ldots,\ m-1$, т.е. полную систему вычетов по модулю m. Так как $(m,\ n) = 1$ (по условию), то по теореме 10 каждый столбец, независимо от k, образует полную систему вычетов по модулю m и содержит потому $\varphi(m)$ чисел, взаимно простых с m.

Итак, всего в таблице имеется $\varphi(m) \cdot \varphi(n)$ чисел, взаимно простых одновременно с m и n, а значит, и с $m \cdot n$, так что $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$. Теорема доказана.

Теперь выведем формулу для вычисления функции Эйлера $\varphi(m)$.

Т е о р е м а 15.

1. *Если* $m = p$ *— простое число, то* $\varphi(m) = p - 1$.

2. *Если* $m = p^\alpha$ *— степень простого числа, то* $\varphi(m) = p^{\alpha-1}(p-1)$.

3. *Если* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *— любое натуральное число, представленное в каноническом разложении, то*

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right).$$

Д о к а з а т е л ь с т в о.

1. Так как p — простое число, то $\forall a \in \mathbb{Z}$ $(a, p) = 1$ или $a \vdots p$ (см. «Алгебра», часть 1). Но из чисел ряда $1, 2, \ldots, p-1, p$, т.е. чисел, не превосходящих p, будет делиться на p, очевидно, только само число p. Значит, остальные $p-1$ чисел будут взаимно просты с p. Поэтому $\varphi(p) = p - 1$.

2. Пусть теперь $m = p^\alpha$. Для определения $\varphi(p^\alpha)$ мы должны рассмотреть ряд чисел от 1 до p^α, который запишем в следующем виде:

$$1,\ 2,\ \ldots,\ p,\ \ldots,\ 2p,\ \ldots,$$
$$\ldots,\ 3p,\ \ldots,\ p \cdot p,\ \ldots,\ p^{\alpha-1} \cdot p = p^\alpha. \qquad (29)$$

Натуральные делители числа p^α являются степенями p (см. «Предварительные сведения», утверждение 6). Поэтому целое число может иметь общий делитель с p^α, отличный от 1, лишь в случае, когда оно делится на p. Ясно, что ряд (29) содержит $p^{\alpha-1}$ чисел, которые делятся на p и, таким образом, не являются взаимно простыми с p^α; остальные числа этого ряда взаимно простые с p^α. Их число, следовательно:

$$\varphi\big(p^\alpha\big) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}\big(p-1\big).$$

3. Пусть, наконец, m — произвольное натуральное число, представленное в каноническом разложении: $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Множители, входящие в это произведение, взаимно просты (см. «Предварительные сведения», утверждение 5), поэтому, используя свойство мультипликативности функции Эйлера, получим:

$$\varphi\big(m\big) = \varphi\big(p_1^{\alpha_1}\big) \cdot \varphi\big(p_2^{\alpha_2}\big) \cdot \ldots \cdot \varphi\big(p_k^{\alpha_k}\big).$$

Следовательно,

$$\varphi\big(m\big) = \big(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\big) \cdot \big(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\big) \cdot \ldots \cdot \big(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\big),$$

или в другом виде:

$$\varphi(m) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) =$$

$$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) =$$

$$= m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Теорема доказана.

З а д а ч а 1. Вычислить а) $\varphi(35)$; б) $\varphi(288)$.

Р е ш е н и е.

а) Так как $35 = 5 \cdot 7$, а $(5,\ 7) = 1$, то, воспользовавшись свойством мультипликативности функции Эйлера, получим:

$$\varphi(35) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24.$$

б) Представим число 288 в канонической записи: $288 = 2^5 \cdot 3^2$ (проверьте самостоятельно!). Тогда по п. 3 последней теоремы

$$\varphi(288) = 288\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 288 \cdot \frac{1}{2} \cdot \frac{2}{3} = 96.$$

2. Тождество Гаусса. Для функции Эйлера имеет место тождество:

$$\sum_{d|n} \varphi(n) = n,$$

где суммирование в левой части распространено на все делители d числа n. Его называют *тождеством Гаусса.*

Чтобы доказать это тождество, применим к $\varphi(n)$ общее тождество для мультипликативных числовых функций:

$$\sum_{d|n} \varphi(n) = [1 + \varphi(p_1) + \varphi(p_1^2) + \ldots + \varphi(p_1^{\alpha_1})] \times$$

$$\times [1 + \varphi(p_2) + \varphi(p_2^2) + \ldots + \varphi(p_2^{\alpha_2})] \times \ldots \times$$

$$\times [1 + \varphi(p_k) + \varphi(p_k^2) + \ldots + \varphi(p_k^{\alpha_k})],$$

где $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ (см. формулу (1)).

Согласно теореме 15 получим:

$$\sum_{d|n} \varphi(n) = [1 + (p_1 - 1) + (p_1^2 - p_1) + (p_1^3 - p_1^2) + \ldots + (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})] \times$$

$$\times [1 + (p_2 - 1) + (p_2^2 - p_2) + (p_2^3 - p_2^2) + \ldots + (p_2^{\alpha_2} - p_2^{\alpha_2 - 1})] \times \ldots \times$$

$$\times [1 + (p_k - 1) + (p_k^2 - p_k) + (p_k^3 - p_k^2) + \ldots + (p_k^{\alpha_k} - p_k^{\alpha_k - 1})] =$$

$$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = n.$$

Тождество Гаусса доказано.

П р и м е р. Пусть $n = 18$. Составим таблицу:

d	1	2	3	6	9	18
$\varphi(d)$	1	1	2	2	6	6

Тогда

$$\sum_{d|20} \varphi(n) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) =$$

$$= 1 + 1 + 2 + 2 + 6 + 6 = 18.$$

3. Теоремы Эйлера и Ферма. Следующая теорема была доказано Л. Эйлером в 1760 году и носит его имя.

Т е о р е м а 16 (Э й л е р а). *Для каждого целого числа a, взаимно простого с модулем m, выполняется сравнение*

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

Д о к а з а т е л ь с т в о. Используем для доказательства свойство приведенной системы вычетов (теорема 13).

Пусть $r_1,\ r_2,\ \ldots,\ r_{\varphi(m)}$ — какая-нибудь приведенная система вычетов по модулю m. Тогда и числа

$$ar_1,\ ar_2,\ \ldots,\ ar_{\varphi(m)}$$

также образуют приведенную систему вычетов по модулю m.

Числа как первой, так и второй совокупности распределены среди $\varphi(m)$ классов чисел, взаимно простых с модулем m. Поэтому между числами первой совокупности и числами второй совокупности можно установить взаимно-однозначное соответствие, при котором соответствующие числа лежат в одном классе вычетов по модулю m, а значит, сравнимы по модулю m, т.е.

$$\begin{array}{lcll} ar_1 & \equiv & r_{i_1} & (\mathrm{mod}\ m); \\ ar_2 & \equiv & r_{i_2} & (\mathrm{mod}\ m); \\ \ldots & \ldots & \ldots & \ldots\ldots\ldots; \\ ar_{\varphi(m)} & \equiv & r_{i_{\varphi(m)}} & (\mathrm{mod}\ m). \end{array}$$

Здесь $r_{i_1},\ r_{i_2},\ \ldots,\ r_{i_{\varphi(m)}}$ — это все те же числа, что и $r_1,\ r_2,\ \ldots,\ r_{\varphi(m)}$, но только, может быть, записанные в другом порядке (см. замечание к теореме 13).

Перемножив почленно эти сравнения, получим:

$$a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv r_{i_1} \cdot r_{i_2} \cdot \ldots \cdot r_{i_{\varphi(m)}} \pmod{m}.$$

Но так как произведения $r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}$ и $r_{i_1} \cdot r_{i_2} \cdot \ldots \cdot r_{i_{\varphi(m)}}$ по предыдущему равны и, кроме того, взаимно просты с модулем, ибо каждый их сомножитель взаимно прост с модулем (см. «Предварительные сведения», утверждение $4'$), то можно обе части сравнения разделить на них, после чего получаем утверждение теоремы Эйлера $a^{\varphi(m)} \equiv 1 \pmod{m}$. Теорема доказана.

Особенно простой вид теорема Эйлера принимает, если $m = p$ — простое число. В этом случае $\varphi(p) = p - 1$, а потому получаем следующее утверждение:

Т е о р е м а 17 (м а л а я т е о р е м а Ф е р м а). *Если p — простое число и a — целое число, такое что $(a\ , p) = 1$, то*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Часто применяется следующее следствие малой теоремы Ферма:

С л е д с т в и е. *Если p — простое число, то для любого целого числа a имеет место сравнение*

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

Д о к а з а т е л ь с т в о.

а) Если $(a,\ p) = 1$, то согласно теореме Ферма $a^{p-1} \equiv \equiv 1 \pmod{p}$. После умножения обеих частей этого сравнения на a, получим: $a^p \equiv a \pmod{p}$.

б) Если $(a,\ p) \neq 1$, то $a \vdots p$ (см. «Алгебра», часть 1). Но тогда и произведение $a(a^{p-1} - 1) = a^p - a$ тоже делится на p, т.е. $a^p - a \equiv 0 \pmod{p}$, или $a^p \equiv a \pmod{p}$.

Итак, $\forall a \in \mathbb{Z}$ имеем: $a^p \equiv a \pmod{p}$. Следствие доказано.

Рассмотрим некоторые задачи на применение теоремы Эйлера и малой теоремы Ферма.

З а д а ч а 2. Найти две последние цифры числа 243^{402}.

Р е ш е н и е. Очевидно, достаточно найти остаток, полученный при делении числа 243^{402} на 100. Так как $243 \equiv 43 \pmod{100}$, то по следствию свойства 3 сравнений

$$243^{402} \equiv 43^{402} \pmod{100}.$$

Но $(43,\ 100) = 1$, а поэтому

$$43^{\varphi(100)} \equiv 1 \pmod{100}.$$

Найдем $\varphi(100)$:

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$$

Таким образом,

$$43^{40} \equiv 1 \pmod{100}.$$

Возведем это сравнение почленно в десятую степень:

$$43^{400} \equiv 1 \pmod{100}.$$

Возьмем сравнение

$$43^2 \equiv 49 \pmod{100};$$

перемножая последние два сравнения, получим:

$$43^{402} \equiv 49 \pmod{100}.$$

Следовательно, искомый остаток равен 49.

З а д а ч а 3. Найти остаток от деления 2^{30} на 13.

Р е ш е н и е. 13 — простое число. Числа 2 и 13 взаимно просты, а поэтому из малой теоремы Ферма следует, что

$$2^{12} \equiv 1 \pmod{13}.$$

Возводя в квадрат почленно последнее сравнение, получим:

$$2^{24} \equiv 1 \pmod{13}.$$

Умножая это сравнение на вспомогательное сравнение

$$2^6 \equiv 2^6 \pmod{13},$$

придем к сравнению:

$$2^{30} \equiv 64 \pmod{13}$$

или, прибавив к правой части число -52, кратное модулю:

$$2^{30} \equiv 12 \pmod{13}.$$

Значит, искомый остаток равен 12.

З а д а ч а 4. Показать, что число $13^{176} - 1$ делится на 89.

Р е ш е н и е. Воспользуемся формулой разложения разности квадратов:

$$13^{176} - 1 = \left(13^{88} - 1\right)\left(13^{88} + 1\right).$$

Если хотя бы один из сомножителей, стоящих в правой части этого равенства, делится на 89, то данное число делится на 89.

Так как 89 — простое число и $(13,\ 89) = 1$, то на основании малой теоремы Ферма справедливо сравнение:

$$13^{88} \equiv 1 \pmod{89},$$

откуда $\left(13^{88} - 1\right) \vdots 89$, а следовательно,

$$\left(13^{176} - 1\right) \vdots 89.$$

§4. Арифметические приложения теории сравнений

1. Теоретическое обоснование признаков делимости. Очень часто возникает потребность, не производя самого деления, ответить на вопрос о делимости одного числа на другое. Критерий, устанавливающий необходимое и достаточное условие делимости произвольного натурального числа N на данное натуральное число m, называется признаком делимости на m.

Различают общие признаки, имеющие силу для любого m, и частные — для отдельных значений m. Общий признак выражает правило, посредством которого по цифрам числа N, записанного в системе счисления с основанием g, можно судить о его делимости на другое число m.

Французский математик Блез Паскаль $(1623 - 1662)$ нашел общий признак делимости, который в терминах сравнений может быть сформулирован следующим образом:

Теорема 17 (общий признак делимости Паскаля). *Для того, чтобы число N, записанное в произвольной g-ичной системе счисления в виде:*

$$N = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0,$$

делилось на число m, необходимо и достаточно, чтобы число

$$Q = a_k r_k + a_{k-1} r_{k-1} + \ldots + a_1 r_1 + a_0$$

делилось на m (здесь a_i — цифры числа N, а r_i — абсолютно наименьшие вычеты соответствующих степеней g^i по модулю m, $i = 1,\ 2,\ \ldots,\ n$).

Доказательство. Пусть $g^i \equiv r_i \pmod m$, где r_i — абсолютно наименьший вычет числа g^i по модулю m

$(i = 1,\ 2,\ \ldots,\ n)$. Тогда

$$N = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0 \equiv$$

$$\equiv a_k r_k + a_{k-1} r_{k-1} + \ldots + a_1 r_1 + a_0 \pmod{m}. \qquad (30)$$

Число N делится на m тогда и только тогда, когда

$$N = a_k g^k + a_{k-1} g^{k-1} + \ldots + a_1 g + a_0 \equiv 0 \pmod{m}. \quad (31)$$

Из сравнений (30) и (31) и транзитивности отношения сравнимости получаем условие, равносильное условию (31):

$$Q = a_k r_k + a_{k-1} r_{k-1} + \ldots + a_1 r_1 + a_0 \equiv 0 \pmod{m}. \quad (32)$$

Из доказанного следует вывод: для того, чтобы N делилось на m, необходимо и достаточно, чтобы Q делилось на m. Теорема доказана.

Из этого признака можно получить признак делимости на любое натуральное число в любой системе счисления.

П р и м е р. Пусть основание системы счисления $g = 10$ и $m = 3$. Тогда:

$$\begin{array}{lcll} 10^0 & \equiv & 1 & (\mathrm{mod}\ 3) \\ 10^1 & \equiv & 1 & (\mathrm{mod}\ 3) \\ 10^2 & \equiv & 1 & (\mathrm{mod}\ 3) \\ \ldots & \ldots & \ldots & \ldots\ldots\ldots \\ 10^k & \equiv & 1 & (\mathrm{mod}\ 3). \end{array}$$

Следовательно,

$$\begin{array}{lcll} a_0 \cdot 10^0 & \equiv & a_0 & (\mathrm{mod}\ 3) \\ a_1 \cdot 10^1 & \equiv & a_1 & (\mathrm{mod}\ 3) \\ a_2 \cdot 10^2 & \equiv & a_2 & (\mathrm{mod}\ 3) \\ \ldots\ldots\ldots & \ldots & \ldots & \ldots\ldots\ldots \\ a_k \cdot 10^k & \equiv & a_k & (\mathrm{mod}\ 3). \end{array}$$

Складывая последние сравнения почленно, получим:

$$N \equiv a_0 + a_1 + a_2 + \ldots + a_k \pmod 3,$$

т.е. $N \vdots 3 \Leftrightarrow (a_0 + a_1 + a_2 + \ldots + a_k) \vdots 3$. Другими словами, число N делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

Используя общий признак делимости Паскаля, получите признаки делимости на 4, 5, 7, 9, 10, 11, 13.

2. Проверка результатов арифметических действий. С помощью сравнений легко указать необходимые признаки правильности и достаточные признаки неправильности результатов выполнения арифметических действий сложения, вычитания и умножения целых чисел.

Понятно, что результат действия сложения, вычитания и умножения есть рациональная функция компонент, а потому если вместо данных чисел взять наименьшие положительные или наименьшие по абсолютной величине вычеты этих чисел по какому-либо модулю, то результат действий над этими вычетами должен быть сравним по тому же модулю с наименьшим вычетов проверяемого результата. Если сравнение не имеет места, то результат получен неверно. В качестве модуля удобнее брать число, наименьшие вычеты по которому легко вычисляются (например, для десятичной системы счисления — 9, 11 или 5). В случае 9 можно брать вместо наименьших вычетов просто сумму цифр, в случае 11 — разность между суммами цифр, стоящих на четных и нечетных местах, считая справа налево (докажите справедливость этих фактов самостоятельно!).

Следует отметить, что неправильность соответствующего сравнения гарантирует неправильность выполнения действий. Правильность соответствующего сравнения лишь

подтверждает, но не гарантирует правильность результата. Дело в том, что проверкой с помощью 9 или 11 не может быть обнаружена ошибка на число, кратное 9 или 11 соответственно. Поэтому чаще всего проверяют одновременно числами 9 и 11. В этом случае возможна ошибка на число, кратное 99, но вероятность такой ошибки очень мала.

З а д а ч а 13. Проверить правильность выполнения действий (с помощью 9 и 11): $8740297 - 561245 = 8179052$.

Р е ш е н и е.

а) Проверка девяткой. Заменяем числа суммами их цифр:

$$37 - 23 \equiv 32 \pmod 9, \quad 14 \equiv 32 \pmod 9.$$

Сравнение подтверждает, но не гарантирует правильности выполнения действий.

б) Проверка числом 11.

$$8740297 \equiv (7 + 2 + 4 + 8) - (9 + 0 + 7) \equiv 5 \pmod{11},$$

$$561245 \equiv (5 + 2 + 6) - (4 + 1 + 5) \equiv 3 \pmod{11},$$

$$8179052 \equiv (2 + 0 + 7 + 8) - (5 + 9 + 1) \equiv 2 \pmod{11}.$$

Получим: $5 - 3 \equiv 2 \pmod{11}$, $2 \equiv 2 \pmod{11}$.

Проверка одиннадцатью подтверждает правильность получения результата (хотя абсолютной гарантии нет, так как возможна ошибка на число, кратное 99).

З а д а ч а 14. Проверить правильность выполнения действий (с помощью 9): $375426 \cdot 3846 = 1443888276$.

Р е ш е н и е. Заменяем числа суммами их цифр:

$$27 \cdot 21 \not\equiv 51 \pmod 9.$$

Следовательно, действие выполнено неправильно.

З а м е ч а н и е. Результат деления проверяется с помощью контроля умножения (делимое равно делителю, умноженному на частное, плюс остаток). Вообще следует иметь в виду, что соблюдение контроля при неверных вычислениях связано, по меньшей мере, с двукратной ошибкой в вычислениях, поэтому следует признать контроль (даже одним числом) действенным.

Глава V. Сравнения с неизвестной величиной

§1. Решение сравнений

1. Корни сравнений. Пусть m — натуральное число и

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 —$$

многочлен с целыми коэффициентами, причем a_n не делится на m. Если подставлять вместо x целые числа, то значения многочлена $f(x)$ тоже будут целыми числами.

О п р е д е л е н и е 1. Сравнение вида

$$f(x) \equiv 0 \pmod{m} \tag{33}$$

называется *сравнением с неизвестной величиной степени* n.

Решить сравнение (33) — значит найти все целые значения x, которые ему удовлетворяют. Но если x_1 одно такое число, т.е. $f(x_1) \equiv 0 \pmod{m}$, то по свойству 9 сравнений этому сравнению будут также удовлетворять все числа

$$x \equiv x_1 \pmod{m},$$

т.е. все вычеты, принадлежащие к тому же классу, что и x_1 по модулю m. Поэтому *решением сравнения* принято считать не отдельное число, а целый класс чисел по модулю m, удовлетворяющих данному сравнению (33).

О п р е д е л е н и е 2. *Решить сравнение* (33) — значит найти все классы вычетов по модулю m, удовлетворяющих сравнению (33) или показать, что таковых нет.

З а м е ч а н и е. Таких классов решений сравнение (33) имеет, очевидно, столько, сколько вычетов полной системы ему удовлетворяют.

Иногда мы и отдельные числа называем решениями, но при этом они считаются разными только в том случае, когда они несравнимы друг с другом по данному модулю, т.е. принадлежат разным классам.

Непосредственным испытанием всех вычетов полной системы по модулю m можно установить, какие из них данному сравнению удовлетворяют. Соответствующие им классы по модулю m являются решениями сравнения. Описанный способ нахождения решений называется методом подбора.

Если модуль m достаточно мал, то сравнение (33) можно решить методом подбора.

З а д а ч а 1. Решить сравнение:

$$x^5 + x + 1 \equiv 0 \pmod 7.$$

Р е ш е н и е. Запишем полную систему абсолютно наименьших вычетов по модулю 7: $0, \pm 1, \pm 2, \pm 3$. Надо подставить вместо x эти вычеты. При $x_0 = 2$ получим: $35 \equiv 0 \pmod 7$, поэтому класс $\overline{2}$ есть решение данного сравнения.

На практике указанный выше прием испытания вычетов при больших модулях оказывается громоздким. Естественно возникает вопрос: существуют ли способы (приемы), позволяющие найти все решения сравнения (33) значительно быстрее? Такие способы существуют и опираются на ряд теорем о равносильности сравнений.

2. Равносильность сравнений с одним неизвестным.

О п р е д е л е н и е 3. Два сравнения

$$f(x) \equiv 0 \pmod m \text{ и } g(x) \equiv 0 \pmod m$$

называются *равносильными*, если множества их классов ре-

шений совпадают. Обозначение:

$$\big(f(x) \equiv 0 \pmod m\big) \Leftrightarrow \big(g(x) \equiv 0 \pmod m\big).$$

Т е о р е м а 1. *Если в сравнении*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod m \quad (34)$$

коэффициенты $a_0,\ a_1, \ldots,\ a_n$ *заменить числами, сравнимыми с ними по модулю* m*, то полученное сравнение*

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0 \equiv 0 \pmod m \quad (35)$$

будет равносильно данному.

Д о к а з а т е л ь с т в о. Пусть $a_0 \equiv b_0 \pmod m$, $a_1 \equiv$ $\equiv b_1 \pmod m$, $\ldots$, $a_n \equiv b_n \pmod m$. Умножим эти сравнения соответственно на $\alpha^0,\ \alpha^1,\ \ldots,\ \alpha^n$, где α — какое-нибудь целое число; получим: $a_0\alpha^0 \equiv b_0\alpha^0 \pmod m$, $a_1\alpha^1 \equiv$ $\equiv b_1\alpha^1 \pmod m$, $\ldots$, $a_n\alpha^n \equiv b_n\alpha^n \pmod m$. Складывая последние сравнения почленно, получим: $a_0 + a_1\alpha^1 + \ldots +$ $+a_n\alpha^n \equiv b_0 + b_1\alpha^1 + \ldots + b_n\alpha^n \pmod m$, или, кратко, $f(\alpha) \equiv$ $\equiv g(\alpha) \pmod m$. Обе части этого сравнения могут быть сравнимы с нулем по модулю m лишь одновременно, а это означает, что сравнения (34) и (35) равносильны. Теорема доказана.

З а м е ч а н и е. Из теоремы 1 следует, что:

а) все коэффициенты сравнения (34), которые делятся на m, можно заменить нулями и вычеркнуть соответствующие члены сравнения;

б) другие коэффициенты можно заменить наименьшими неотрицательными или абсолютно наименьшими вычетами по модулю m.

Например, сравнения $16x^5 + 12x^4 - 3x^3 - x + 3 \equiv 0 \pmod 4$, $-3x^3 - x + 3 \equiv 0 \pmod 4$ и $x^3 - x - 1 \equiv 0 \pmod 4$ равносильны.

О п р е д е л е н и е 4. *Степенью сравнения*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}$$

называют наивысший показатель степени, коэффициент при котором не делится на m.

П р и м е ры. Найдем степени сравнений:

а) Сравнение $2x^3 - 3x + 4 \equiv 0 \pmod 5$ имеет степень $n = 3$, так как 2 не делится на 5, т.е. $2 \not\equiv 0 \pmod 5$.

б) Сравнение $16x^5 + 12x^4 - 3x^3 - x + 3 \equiv 0 \pmod 4$ имеет степень $n = 3$, так как $16 \equiv 0 \pmod 4$, $12 \equiv 0 \pmod 4$, а $-3 \not\equiv 0 \pmod 4$.

Сравнение, у которого все коэффициенты делятся на модуль m, рассматривается, как не имеющее степени. Такому сравнению удовлетворяет любое целое число. Например, сравнение $28x^2 + 7x + 14 \equiv 0 \pmod 7$ степени не имеет. Ему удовлетворяет любое целое число, так как при любом $x \in \mathbb{Z}$ левая часть делится на 7.

При решении сравнений, содержащих неизвестную величину, иногда приходится умножать обе части сравнения на одно и то же число. Однако такое преобразование не всегда приводит к равносильному сравнению. Справедлива

Т е о р е м а 2. *Если обе части сравнения* (34) *умножить на целое число k, взаимно простое с модулем m, то полученное сравнение будет равносильно данному.*

Д о к а з а т е л ь с т в о. Пусть $c \in \overline{c}$ — любое решение сравнения (34), т.е.

$$f(c) = a_n c^n + a_{n-1} c^{n-1} + \ldots + a_1 c + a_0 \equiv 0 \pmod{m}.$$

Умножим обе части сравнения на k, получим:

$$kf(c) = ka_n c^n + ka_{n-1} c^{n-1} + \ldots + ka_1 c + ka_0 \equiv 0 \pmod{m}.$$

Следовательно, $\overline{c}$ — решение сравнения

$$kf(x) \equiv 0 \pmod{m}.$$

Обратно, пусть $d \in \overline{d}$ — решение последнего сравнения, т.е.

$$kf(d) \equiv 0 \pmod{m}.$$

Так как $(k,\ m) = 1$, то обе части этого сравнения можно разделить на k. Получим: $f(d) \equiv 0 \pmod{m}$. Отсюда следует, что $\overline{d}$ — решение сравнения (34). Итак, если $(k,\ m) = 1$, то

$$\big(f(x) \equiv 0 \pmod{m}\big) \Leftrightarrow \big(kf(x) \equiv 0 \pmod{m}\big).$$

Теорема доказана.

З а д а ч а 1. Выяснить, равносильны ли сравнения: $3x - 1 \equiv 0 \pmod 5$ и $3x^3 + 4x^2 + x - 2 \equiv 0 \pmod 5$.

Р е ш е н и е. Запишем полную систему наименьших неотрицательных вычетов по модулю 5: 0, 1, 2, 3, 4. Найдем все классы решений первого и второго сравнения. Первое сравнение имеет единственное решение $\overline{2} = \{x = 2+ +3t,\ t \in \mathbb{Z}\}$, которое является единственным корнем второго сравнения (проверьте это самостоятельно!). Следовательно, данные сравнения равносильны.

З а м е ч а н и е. В этой задаче мы видим, что равносильные сравнения не обязательно должны иметь одну и ту же степень.

Если модуль $m = p$ — простое число, то для понижения степени сравнения можно воспользоваться теоремой Ферма. Действительно, если $(x,\ p) = 1$, то

$$x^{p-1} \equiv 1 \pmod{m} \Rightarrow x^p \equiv x \pmod{m}.$$

П р и м е р. Заменить сравнение

$$3x^{10} + 6x^8 + 3x^6 - 2x^5 - x^3 + 8x - 2 \equiv 0 \pmod 5$$

равносильным сравнением более низкой степени.

Так как $x^5 \equiv x \pmod 5$, то $x^6 \equiv x^2 \pmod 5$, $x^8 \equiv x^4 \pmod 5$, $x^{10} \equiv x^2 \pmod 5$, и потому данное сравнение будет равносильно сравнению

$$x^4 - x^3 + x^2 + x - 2 \equiv 0 \pmod 5.$$

§2. Сравнение первой степени с одной переменной

1. Решение сравнений первой степени. Рассмотрим частный случай сравнения $f(x) \equiv 0 \pmod m$, когда $\deg f(x) = 1$. В этом случае оно будет иметь вид:

$$ax \equiv b \pmod m. \tag{36}$$

Выясним, сколько классов решений может иметь это сравнение.

Т е о р е м а 3. *Если* $(a,\ m) = 1$, *то сравнение* (36) *имеет единственный класс решений.*

Д о к а з а т е л ь с т в о. Рассмотрим какую-нибудь полную систему вычетов по модулю m:

$$x_1,\ x_2, \ldots,\ x_m. \tag{37}$$

По условию $(a,\ m) = 1$. Тогда согласно теореме 10 из п.2 §2 гл. IV совокупность чисел:

$$ax_1,\ ax_2,\ \ldots,\ ax_m$$

тоже полная система вычетов по модулю m. Таким образом, если в (36) вместо x подставлять последовательно все

вычеты полной системы вычетов (37), то левая часть этого сравнения пробегает все значения полной системы вычетов. Но это означает, что для одного x_i $(1 \leqslant i \leqslant m)$ число ax_i окажется в том же самом классе, к которому принадлежит число b; при этом $ax_i \equiv b \pmod{m}$. Итак, если $(a,\ m) = 1$, то сравнение (36) имеет и притом единственное решение

$$x \equiv x_i \pmod{m}.$$

Теорема доказана.

Решение сравнения (36) можно найти путем испытания полной системы абсолютно наименьших вычетов. Для нахождения решения сравнения (36) можно воспользоваться следующей теоремой.

Т е о р е м а 4. *Если* $(a,\ m) = 1$, *то решением сравнения* (36) *является класс* $x \equiv ba^{\varphi(m)-1} \pmod{m}$.

Д о к а з а т е л ь с т в о. По условию $(a,\ m) = 1$, тогда согласно теореме Эйлера $a^{\varphi(m)} \equiv 1 \pmod{m}$. Умножим левую и правую части этого сравнения на b. Получим: $a^{\varphi(m)}b \equiv b \pmod{m}$ или $a \cdot a^{\varphi(m)-1}b \equiv b \pmod{m}$. Сравнивая последнее сравнение с $ax \equiv b \pmod{m}$, находим, что класс $x \equiv ba^{\varphi(m)-1} \pmod{m}$ является решением сравнения $ax \equiv b \pmod{m}$, а согласно теореме 3 это решение единственно. Теорема доказана.

Т е о р е м а 5. *Если* $(a,\ m) = d > 1$ *и* $b \not\vdots d$, *то сравнение* (36) *решений не имеет.*

Д о к а з а т е л ь с т в о. Предположим, что сравнение $ax \equiv b \pmod{m}$ имеет решение — класс $\bar{c}$ по модулю m и $c \in \bar{c}$, тогда $ac \equiv b \pmod{m}$, или $ac = b + mt,\ t \in \mathbb{Z} \Rightarrow$ $\Rightarrow ac - mt = b$. Так как $(a \vdots d)\ \ \&\ \ (m \vdots d)$, то $(ac - mt) \vdots d$, откуда $b \vdots d$, что противоречит условию. Полученное противоречие доказывает теорему.

Т е о р е м а 6. *Если* $(a,\ m) = d > 1$ *и* $b \vdots d$, *то сравнение* (36) *имеет* d *различных решений. Все эти решения образуют один класс по модулю* $\dfrac{m}{d}$.

Д о к а з а т е л ь с т в о. По условию каждое из чисел $a,\ b,\ m$ делится на d. Положим, $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. Разделив обе части сравнения (36) и модуль на d, получим равносильное ему сравнение:

$$a_1 x \equiv b_1 \pmod{m_1}. \tag{38}$$

Действительно, пусть $x = \alpha$ — целое число, удовлетворяющее сравнению (36); тогда $a\alpha \equiv b \pmod{m}$, а после деления обеих частей сравнения и модуля на d получим: $a_1\alpha \equiv$ $\equiv b_1 \pmod{m_1}$. Следовательно, α удовлетворяет сравнению (38).

Обратно, пусть $x = \beta$ удовлетворяет сравнению (38), тогда $a_1\beta \equiv b_1 \pmod{m_1}$. Умножив обе части и модуль этого сравнения на d, получим: $a\beta \equiv b \pmod{m}$. Значит, β удовлетворяет сравнению (36).

Таким образом, сравнения (36) и (38) равносильны.

В сравнении (38) $(a_1,\ m_1) = 1$, поэтому оно имеет единственное решение $x \equiv \pmod{m_1}$, или $x = + m_1 t$, (где c — наименьший неотрицательный вычет по модулю m_1, $t \in \mathbb{Z}$), или

$$\begin{gathered} \ldots,\ c - 2m_1,\ c - m_1,\ c,\ c + m_1,\ c + 2m_1,\ \ldots, \\ \ldots,\ c + (d-1)m_1,\ c + dm_1,\ \ldots \end{gathered} \tag{39}$$

Все вычеты из (39) и только они удовлетворяют сравнению (38) и равносильному ему сравнению (36).

Понятно, что по модулю $m_1 = \dfrac{m}{d}$ все числа из последовательности (39) принадлежат одному классу. По модулю

же $m = m_1 d$ они будут принадлежать различным классам, вычетами которых являются:

$$c,\ c + m_1,\ c + 2m_1,\ \ldots,\ c + (d-1)m_1. \qquad (40)$$

Действительно, разность любых двух вычетов из (40) не делится на m (поэтому все они принадлежат различным классам по модулю m), а для каждого другого вычета из (39) найдется среди вычетов (40) такой, что их разность будет кратна m (поэтому такие вычеты принадлежат одному классу по модулю m).

Следовательно, сравнение (36) имеет d различных решений по модулю m:

$$\begin{array}{lcll} x & \equiv & c & (\mathrm{mod}\ m) \\ x & \equiv & c + m_1 & (\mathrm{mod}\ m) \\ x & \equiv & c + 2m_1 & (\mathrm{mod}\ m) \\ \ldots & \ldots & \ldots\ldots\ldots & \ldots\ldots\ldots \\ x & \equiv & c + (d-1)m_1 & (\mathrm{mod}\ m), \end{array}$$

где c — наименьший неотрицательный вычет из класса — решения сравнения (38). Теорема доказана.

З а д а ч а 2. Решить сравнения:

а) $5x \equiv 3 \pmod 7$;

б) $45x \equiv 14 \pmod{35}$;

в) $8x \equiv 4 \pmod{12}$.

Р е ш е н и е.

а) Так как $(5,\ 7) = 1$, то по теореме 3 сравнение имеет единственный класс решений $x \equiv 3 \cdot 5^{\varphi(7)-1} \pmod 7 \Leftrightarrow x \equiv$ $\equiv 3 \cdot 5^5 \pmod 7 \Leftrightarrow x \equiv 2 \pmod 7 \Rightarrow x = 2 + 7t,\ t \in \mathbb{Z}$.

б) Так как $(45,\ 35) = 5$, но $14 \not\vdots 5$, то сравнение решений не имеет.

в) Так как $(8,\ 4) = 4$ и $4 \vdots 4$, то сравнение имеет четыре решения. Делим обе части и модуль сравнения на 4,

получим: $2x \equiv 1 \pmod 3$. Так как $(2,\ 3) = 1$, то $x \equiv$ $\equiv 2 \pmod 3 \Rightarrow x = 2 + 3t, t \in \mathbb{Z}$. Таким образом, решениями сравнения $8x \equiv 4 \pmod{12}$ будут:

$$\begin{aligned} x_0 &\equiv 2 \pmod{12} \\ x_1 &\equiv 5 \pmod{12} \\ x_2 &\equiv 8 \pmod{12} \\ x_3 &\equiv 11 \pmod{12}. \end{aligned}$$

2. Диофантовы уравнения.

О п р е д е л е н и е 5. Уравнение вида:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{41}$$

где $a_i, x_i \in \mathbb{Z}\ (i = 1,\ 2,\ \ldots,\ n), b \in \mathbb{Z}$, называется *диофантовым уравнением* первой степени с n переменными.

О п р е д е л е н и е 6. Упорядоченный набор целых чисел $(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n)$, удовлетворяющий уравнению (41), называется *решением диофантова уравнения.*

Рассмотрим частный случай уравнения (41):

$$ax + by = c, \tag{42}$$

где $a,\ b,\ c \in \mathbb{Z}$.

Покажем, что отыскание целочисленных решений диофантова уравнения (42) тесно связано с решением сравнений первой степени. Ограничимся рассмотрением случая, когда числа a и b отличны от нуля (если, например, $b = 0$, то уравнение (42) принимает вид $ax = c$).

Итак, пусть $(a \neq 0)\ \ \&\ \ (b \neq 0)$, а пара целых чисел $(x_0,\ y_0)$ — есть одно из решений уравнения (42). Тогда $ax_0 + by_0 = c \Rightarrow ax_0 - c = -by_0 \Rightarrow (ax_0 - c) \vdots b \Rightarrow ax_0 \equiv$ $\equiv c \pmod b$, т.е. x_0 есть решение сравнения (42).

Обратно, пусть x_0 — решение сравнения $ax \equiv c \pmod{b}$. Тогда $ax_0 \equiv c \pmod{b}$, т.е. $(ax_0 - c) \vdots b$. Это значит, что $ax_0 - c = -by_0$, где y_0 — целое число, такое, что $ax_0 + by_0 = c$. Иными словами, $(x_0,\ y_0)$ — целочисленное решение уравнения (42).

Мы доказали следующее утверждение:

Т е о р е м а 7. *Если $(x_0,\ y_0)$ — целочисленное решение диофантова уравнения (42), причем $(a \neq 0)\ \&\ (b \neq 0)$, то x_0 — решение сравнения $ax \equiv c \pmod{b}$.*

Обратно, если x_0 — решение сравнения $ax \equiv c \pmod{b}$, то существует такое $y_0 \in \mathbb{Z}$, что $(x_0,\ y_0)$ — решение диофантова уравнения (42).

Теорема 7 позволяет свести решение диофантовых уравнений вида (42) к решению уравнений первой степени, и обратно.

Поэтому из теорем 3, 5, 6 следует, что уравнение (42) будет иметь решение, если $(a,\ b) = d$ и $c \vdots d$, и не будет иметь решения, если $(a,\ b) = d$ и $c \not\vdots d$.

Процесс нахождения целочисленных решений уравнения вида (42) распадается на два этапа: нахождение хотя бы одного такого решения и нахождение общего вида решений. Рассмотрим сначала второй этап.

Т е о р е м а 8. *Если известно частное целочисленное решение $(x_0,\ y_0)$ диофантова уравнения (42) и $(a,\ b) = d$, то общее решение этого уравнения имеет вид:*

$$x = x_0 - \frac{b}{d}\,t, \qquad y = y_0 + \frac{a}{d}\,t, \tag{43}$$

где t пробегает множество целых чисел.

Д о к а з а т е л ь с т в о. Покажем сначала, что $\forall t \in \mathbb{Z}$

числа $x = x_0 - \dfrac{b}{d}\,t$ и $y = y_0 + \dfrac{a}{d}\,t$ удовлетворяют уравнению (42). В самом деле, так как $(x_0,\ y_0)$ — одно из решений уравнения (42), то $ax_0 + by_0 = c$, и потому

$$a\left(x_0 - \frac{b}{d}\,t\right) + b\left(y_0 + \frac{a}{d}\,t\right) = ax_0 + by_0 = c.$$

Значит, $\forall t \in \mathbb{Z}$ выражения (43) дают решение уравнения (42).

Покажем теперь, что этим исчерпываются все целочисленные решения диофантова уравнения (42). В самом деле, пусть $(x_1,\ y_1)$ — такое решение. Тогда $ax_1 + by_1 = c$ и $ax_0 + by_0 = c$. Вычитая почленно эти равенства, получаем:

$$a(x_1 - x_0) + b(y_1 - y_0) = 0. \tag{44}$$

Так как $(a,\ b) = d$, то числа $\dfrac{a}{d}$ и $\dfrac{b}{d}$ взаимно просты. Поделим обе части последнего равенства на d и перенесем второе слагаемое в правую часть:

$$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0).$$

Но $\dfrac{a}{d}$ и $\dfrac{b}{d}$ взаимно просты, а левая часть равенства делится на $\dfrac{a}{d}$. Поэтому $(y_1 - y_0) \vdots \dfrac{a}{d} \Rightarrow y_1 - y_0 = \dfrac{a}{d}\,t_1 \Rightarrow y_1 = y_0 + \dfrac{a}{d}\,t_1$, $t_1 \in \mathbb{Z}$. Подставляя значение $y_1 - y_0 = \dfrac{a}{d}\,t_1$ в (44), получаем:

$$\frac{a}{d}\,(x_1 - x_0) = -\frac{b}{d} \cdot \frac{a}{d} \cdot t_1,$$

и потому

$$x_1 - x_0 = -\frac{b}{d}\,t_1 \Rightarrow x_1 = x_0 - \frac{b}{d}\,t_1.$$

Мы нашли такое целое t_1, что

$$(x_1 = x_0 - \frac{b}{d}\,t_1) \;\&\; (y_1 = y_0 + \frac{a}{d}\,t_1).$$

Теорема доказана.

В частном случае, когда a и b взаимно просты, формулы общего решения (43) принимают вид:

$$x = x_0 - bt, \qquad y = y_0 + at \tag{45}$$

Для нахождения частных решений применимы те же способы, что и для решения сравнений (можно использовать, к примеру, теорему Эйлера).

З а д а ч а 3. Решить диофантово уравнение:

$$8x + 6y = 4.$$

Р е ш е н и е. Поделив обе части уравнения на 2, получим равносильное уравнение: $4x + 3y = 2$. Заменим это уравнение сравнением: $4x \equiv 2 \pmod 3$. Решая его, находим: $x \equiv 2 \pmod 3 \Rightarrow x = 2 + 3t, t \in \mathbb{Z}$. Теперь найдем общее решение уравнения: $x = 2 + 3t \Rightarrow 8(2 + 3t) + 6y = = 4 \Rightarrow 6y = 4 - 16 - 24t \Rightarrow y = -2 - 4t$.

Итак, $x = 2 + 3t; y = -2 - 4t, t \in \mathbb{Z}$.

З а д а ч а 4. Решить диофантово уравнение:

$$5x + 3y = 7.$$

Р е ш е н и е. Запишем уравнения в виде сравнения: $5x \equiv 7 \pmod 3$, откуда $x \equiv 2 \pmod 3$, т.е. $x = 2+3t, t \in \mathbb{Z}$. Подставим найденное выражение для x в уравнение. Получим: $5(2+3t)+3y = 7 \Rightarrow 3y = 7-5(2+3t) \Rightarrow 3y = -3-15t \Rightarrow \Rightarrow y = -1 - 5t$.

Таким образом, $x = 2 + 3t; y = -1 - 5t, t \in \mathbb{Z}$.

З а м е ч а н и е. Если в диофантовом уравнении (42) $(a,\ b) = 1$ и $a,\ b \in \mathbb{N}$, то его можно решить с помощью цепных дробей.

Разложим $\dfrac{a}{b}$ в цепную дробь: $\dfrac{a}{b} = [q_0;\ q_1,\ \ldots,\ q_n]$ и найдем подходящие дроби. Последняя подходящая дробь $\dfrac{P_n}{Q_n} = \dfrac{a}{b}$.

Так как по условию $(a,\ b) = 1$ и $(P_n,\ Q_n) = 1$ (по теореме 6 п.2 §1 гл. III), то $P_n = a$, $Q_n = b$.

Согласно теореме 5 п.2 §1 гл. III имеем:

$$P_{n-1}Q_n - P_nQ_{n-1} = (-1)^n,$$

или

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n-1},$$

или

$$aQ_{n-1} - bP_{n-1} = (-1)^{n-1}.$$

Умножая обе части последнего равенства на $(-1)^{n-1}c$, получим

$$a(-1)^{n-1}cQ_{n-1} + b(-1)^ncP_{n-1} = c. \qquad (46)$$

Сравнивая (46) с (42), находим частное решение уравнения (42):

$$x_0 = (-1)^{n-1}cQ_{n-1}, \qquad y_0 = (-1)^ncP_{n-1}. \qquad (47)$$

Из (45) и (47) следует, что общее решение уравнения имеет вид:

$$x = (-1)^{n-1}cQ_{n-1} - bt, \qquad y = (-1)^ncP_{n-1} + at, \qquad (48)$$

где P_{n-1} и Q_{n-1} — числитель и знаменатель предпоследней подходящей дроби разложения $\dfrac{a}{b}$ в цепную дробь, а t — любое целое число.

З а д а ч а 5. Решить диофантово уравнение

$$3x + 7y = 11$$

с помощью цепных дробей.

Р е ш е н и е. Здесь $a = 3$, $b = 7$, $c = 11$. Разложим $\frac{3}{7}$ в цепную дробь: $\frac{3}{7} = [0;\ 2,\ 3]$. Имеем: $n = 2$, $P_{n-1} = P_1 = 1$, $Q_{n-1} = Q_1 = 2$; одним из частных решений будет:

$$x_0 = (-1)^1 \cdot 11 \cdot 2 = -22, \qquad y_0 = (-1)^0 \cdot 11 \cdot 1 = 11.$$

Общее решение согласно (48) будет:

$$x = -22 - 7t, \qquad y = 11 + 3t, \qquad t \in \mathbb{Z}.$$

§3. Системы сравнений первой степени с одной переменной

1. Решение систем сравнений первой степени.

О п р е д е л е н и е 7. Система вида:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \dots \quad \dots \quad \dots \qquad \dots\dots\dots \\ a_k x \equiv b_k \pmod{m_k} \end{cases} \tag{49}$$

называется *системой сравнений первой степени с одной переменной.*

Если некоторое число α удовлетворяет этой системе, т.е. если $(a_1\alpha - b_1) \vdots m_1$, $(a_2\alpha - b_2) \vdots m_2$, $\dots$, $(a_k\alpha - b_k) \vdots m_k$ и $M = [m_1,\ m_2,\ \dots,\ m_k]$ — наименьшее общее кратное чисел $m_1,\ m_2,\ \dots,\ m_k$, а β — любое число, такое, что $\beta \equiv$

$\equiv \alpha \pmod{M}$, то (свойство 9 п.2 §1 гл. IV) для всех i $(1 \leqslant i \leqslant k)$ будет $a_i\beta - b_i \equiv a_i\alpha - b_i \pmod{M}$, а, следовательно (свойство 5 п.2 §1 гл. IV), $a_i\beta - b_i \equiv a_i\alpha - b_i \pmod{m_i}$, т.е. $a_i\beta - b_i \equiv 0 \pmod{m_i}$, или $a_i\beta \equiv b_i \pmod{m_i}$, $(1 \leqslant i \leqslant k)$.

Мы видим, что вместе с каждым числом α, удовлетворяющим системе (49), этой же системе удовлетворяет и любое число класса $\overline{\alpha}$ по модулю $M = [m_1, m_2, \ldots, m_k]$. Естественно весь этот класс чисел рассматривать как одно решение этой системы.

О п р е д е л е н и е 8. *Решением системы сравнений* (49) называется класс чисел по модулю $M = [m_1, m_2, \ldots, m_k]$, состоящий из чисел, удовлетворяющих каждому сравнению системы.

О п р е д е л е н и е 9. Система (49) называется *совместной*, если она имеет хотя бы одно решение (класс решений).

З а м е ч а н и е. Если хотя бы одно сравнение системы (49) не будет иметь решения, то и вся система (49) будет несовместной.

2. Количество решений системы сравнений. Решить систему (49) — значит найти все целые значения x, которые ей удовлетворяют. Ясно, что для существования таких чисел необходимо (но недостаточно), чтобы каждое сравнение в отдельности было разрешимым. Поэтому достаточно ограничиться рассмотрением системы

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \ldots \quad \ldots \quad \ldots \quad \ldots\ldots\ldots \\ x \equiv c_k \pmod{m_k}. \end{cases} \tag{50}$$

Рассмотрим сначала систему вида:

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2}. \end{cases} \tag{51}$$

Для краткости будем называть эти сравнения соответственно первым и вторым.

Т е о р е м а 9. *Пусть d — наибольший общий делитель, а M — наименьшее общее кратное m_1 и m_2; тогда, если $(c_2 - c_1) \not\vdots d$, то система сравнений* (51) *не имеет решений, а если $(c_2 - c_1) \vdots d$, то система* (51) *имеет единственное решение, представляющее собой класс чисел по модулю M.*

Д о к а з а т е л ь с т в о. Из первого сравнения (51) получаем $x = c_1 + m_1 t$. При любом целом t такие x удовлетворяют первому сравнению. Задача нахождения решений системы (51) сводится, таким образом, к тому, чтобы выбрать такие t, при которых x удовлетворяет и второму сравнению, т.е. найти все целые t, такие, что

$$c_1 + m_1 t \equiv c_2 \pmod{m_2}.$$

Отыскание таких t свелось к решению сравнения первой степени с неизвестной t:

$$m_1 t \equiv c_2 - c_1 \pmod{m_2}. \tag{52}$$

Если при $(m_1,\ m_2) = d$ будет $(c_2 - c_1) \not\vdots d$, то (теорема 5) сравнение (52) не имеет решений, т.е. среди всех значений x, удовлетворяющих сравнению $x \equiv c_1 \pmod{m_1}$, нет ни одного, которое удовлетворяло бы сравнению $x \equiv c_2 \pmod{m_2}$, и система (51) несовместна. Если $(c_2 - c_1) \vdots d$, то решение сравнения (52) можно записать (теорема 6) в виде класса по модулю $\dfrac{m_2}{d}$, т.е. в виде:

$$t \equiv \alpha \pmod{\frac{m_2}{d}}, \quad t = \alpha + \frac{m_2}{d} y, \quad y \in \mathbb{Z};$$

подставляя эти значения t в уравнение ($x = c_1 + m_1 t$), выделяем из множества значений x, удовлетворяющих первому сравнению, те, которые удовлетворяют и второму:

$$x = c_1 + m_1\left(\alpha + \frac{m_2}{d} y\right) = c_1 + m_1\alpha + \frac{m_1 m_2}{d} y = \beta + \frac{m_1 m_2}{d} y,$$

$$y \in \mathbb{Z}.$$

Эти значения x образуют класс по модулю $\dfrac{m_1 m_2}{d} = M$, т.е. $x \equiv \beta \pmod{M}$.

В соответствии с определением 8 система сравнений имеет одно решение. Теорема доказана.

Т е о р е м а 10. *Система сравнений* (50) *либо совсем не имеет решений, либо имеет единственное решение, представляющее собой класс чисел по модулю* M, *равному наименьшему общему кратному чисел* $m_1,\ m_2,\ \ldots,\ m_k$.

Доказательство этой теоремы проведите самостоятельно, используя метод математической индукции (по числу сравнений k).

З а м е ч а н и е. Если система (50) имеет решения, то их можно найти, решив сначала первые два сравнения, добавив потом последовательно третье и т.д., пока не будет исчерпана вся система.

З а д а ч а 6. Исследовать, имеет ли решение система

$$\begin{cases} 2x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{11}. \end{cases}$$

и, если имеет, то найти его.

Р е ш е н и е. Решим первое уравнение системы. Так как $(2,\ 7) = 1$, то получим: $x \equiv 5 \pmod 7$. Система примет вид:

$$\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 4 \pmod{11}. \end{cases}$$

Имеем: $(7,\ 11) = 1 \Rightarrow$ система имеет решение. Находим решение первого сравнения: $x = 5 + 7t$. Подставим выражение для x во второе сравнение системы. Получим: $5 + 7t \equiv$ $\equiv 4 \pmod{11} \Leftrightarrow 7t \equiv -1 \pmod{11}$. Так как $(7,\ 11) =$ $= 1$, то это сравнение имеет единственный класс решений: $t \equiv 3 \pmod{11}$ или $t = 3 + 11u$. Тогда: $x = 5 + 7t =$ $= 5 + 7(3 + 11u) = 5 + 21 + 77u = 26 + 77u, u \in \mathbb{Z}$. Таким образом, $x = 26 + 77u$, $u \in \mathbb{Z}$.

З а д а ч а 7. Решить систему сравнений:

$$\begin{cases} 4x \equiv 2 \pmod 6 \\ x \equiv 3 \pmod 5 \\ x \equiv -2 \pmod 7. \end{cases}$$

Р е ш е н и е. Решим первое сравнение системы. Так как $(4,\ 6) = 2$ и $2 \vdots 2$, то оно имеет два класса решений. Найдем их:

$$4x \equiv 2 \pmod 6 \Leftrightarrow 2x \equiv 1 \pmod 3 \Rightarrow$$

$$\Rightarrow 2x \equiv 4 \pmod 3 \Rightarrow x \equiv 2 \pmod 3 \Leftrightarrow$$

$$\Leftrightarrow x = 2 + 3t, \quad t \in \mathbb{Z},$$

откуда получаем решения первого сравнения:

$$\begin{aligned} x_0 &\equiv 2 \pmod 6 \\ x_1 &\equiv 5 \pmod 6. \end{aligned}$$

Таким образом, исходная система сравнений будет равно-

сильна совокупности двух систем сравнений:

$$\left[\begin{array}{l}\left\{\begin{array}{rcll} x & \equiv & 2 & (\mathrm{mod}\ 6)\\ x & \equiv & 3 & (\mathrm{mod}\ 5)\\ x & \equiv & -2 & (\mathrm{mod}\ 7)\end{array}\right.\\ \left\{\begin{array}{rcll} x & \equiv & 5 & (\mathrm{mod}\ 6)\\ x & \equiv & 3 & (\mathrm{mod}\ 5)\\ x & \equiv & -2 & (\mathrm{mod}\ 7).\end{array}\right.\end{array}\right.$$

Решим сначала первую систему. Из первого сравнения получим: $x = 2 + 6t$; подставляя это выражение во второе сравнение, приходим к сравнению $2 + 6t \equiv 3 \pmod 5 \Rightarrow$ $\Rightarrow 6t \equiv 1 \pmod 5$. Так как $(6,\ 5) = 1$, то $t \equiv 1 \pmod 5 \Rightarrow$ $\Rightarrow t = 1 + 5q$. Подставляем $t = 1 + 5q$ в равенство $x = 2 + 6t$. Получим: $x = 2 + 6(1 + 5q) = 2 + 6 + 30q = 8 + 30q$.

Теперь подставляем $x = 8 + 30q$ в третье сравнение первой системы. Имеем: $8 + 30q \equiv -2 \pmod 7 \Rightarrow$ $\Rightarrow 30q \equiv -10 \pmod 7$. Так как $(30,\ 7) = 1$, то $q \equiv$ $\equiv 2 \pmod 7 \Rightarrow q = 2 + 7p$, где $p \in \mathbb{Z}$. Тогда $x =$ $= 8 + 30q = 8 + 30(2 + 7p) = 68 + 210p$, $p \in \mathbb{Z} \Rightarrow$ $\Rightarrow x \equiv 68 \pmod{210}$.

Итак, решение первой системы: $x \equiv 68 \pmod{210}$.

Решаем вторую систему. Из сравнения $x \equiv 5 \pmod 6$ получаем, что $x = 5 + 6s$. Поэтому $5 + 6s \equiv 3 \pmod 5 \Rightarrow$ $\Rightarrow 6s \equiv -2 \pmod 5 \Rightarrow s \equiv 3 \pmod 5 \Rightarrow s = 3 + 5u$. Тогда $x = 5 + 6s = 5 + 6(3 + 5u) = 5 + 18 + 30u = 23 + 30u$. Имеем: $23 + 30u \equiv -2 \pmod 7 \Rightarrow 30u \equiv -25 \pmod 7$. Так как $(30,\ 7) = 1$, то $u \equiv 5 \pmod 7 \Rightarrow u = 5 + 7v$. Тогда $x = 23 + 30u = 23 + 30(5 + 7v) = 23 + 150 + 210v = 173 + 210v$, $v \in \mathbb{Z} \Rightarrow x \equiv 173 \pmod{210}$.

Итак, решение второй системы: $x \equiv 173 \pmod{210}$.

Таким образом, система имеет два класса решений:

$$\begin{aligned} x_0 &\equiv 68 \pmod{210} \\ x_1 &\equiv 173 \pmod{210}. \end{aligned}$$

§4. Сравнения высших степеней по простому модулю

1. О максимальном числе решений. Сравнения по простому модулю представляют собой наиболее простой случай сравнений. Вместе с тем это и наиболее важный случай, так как решение сравнения по составному модулю можно свести к решению сравнения по простому модулю.

Во всем этом параграфе буквой p будем обозначать модуль, представляющий собой простое число.

О п р е д е л е н и е 10. Сравнение вида

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}, \quad (53)$$

где $a_n \not\vdots p$, называют *сравнением n-ой степени по простому модулю.*

Общих методов решения сравнения (53) не существует (если не считать перебор полной системы вычетов по модулю p). Существующие же частные приемы решения основаны на понятии равносильности сравнений и теореме Ферма.

Т е о р е м а 11. *Сравнение* (53) *при* $n \geqslant p$ *равносильно некоторому сравнению степени не выше* $p-1$.

Д о к а з а т е л ь с т в о. Пусть дано сравнение (53), причем $\deg f(x) = n \geqslant p$. Имеем: $\forall x \in \mathbb{Z}$ $(x,\ p) = 1$, поэтому имеет место следствие теоремы Ферма: $x^p \equiv x \pmod{p} \Rightarrow (x^p - x) \equiv 0 \pmod{p}$. Разделим многочлен $f(x)$ на многочлен $x^p - x$ с остатком. Получим:

$$f(x) = (x^p - x)q(x) + r(x), \quad \deg r(x) < \deg(x^p - x) = p.$$

Тогда

$$f(x) \equiv 0 \pmod{p} \Leftrightarrow (x^p - x)q(x) + r(x) \equiv 0 \pmod{p}.$$

Учитывая, что $\forall x \in \mathbb{Z} \quad x^p - x \equiv 0 \pmod{p}$, получим:

$$f(x) \equiv 0 \pmod{p} \Leftrightarrow r(x) \equiv 0 \pmod{p},$$

$$\deg r(x) \leqslant (p-1).$$

Теорема доказана.

З а д а ч а 8. Решить сравнение:

$$f(x) = x^8 + 13x^5 + 8x^3 + 10x^2 + 13 \equiv 0 \pmod{5}.$$

Р е ш е н и е. Упростим левую часть сравнения, заменив коэффициенты многочлена $f(x)$ числами, сравнимыми по модулю 5:

$$f(x) \equiv x^8 + 3x^5 + 3x^3 + 3 \equiv 0 \pmod{5}.$$

Поделим многочлен $f(x)$ на многочлен $x^5 - x$ с остатком. Получим: $f(x) = (x^5 - x)(x^3 + 3) + (x^4 + 3x^3 + 3x + 3)$. Тогда

$$x^8 + 13x^5 + 8x^3 + 10x^2 + 13 \equiv 0 \pmod{5} \Leftrightarrow$$

$$\Leftrightarrow x^4 + 3x^3 + 3x + 3 \equiv 0 \pmod{5}.$$

Полученное сравнение решаем методом испытания полной системы вычетов по модулю 5: $0, \pm 1, \pm 2$. Находим, что $x \equiv 1 \pmod{5}$.

Таким образом, $x \equiv 1 \pmod{5}$ — единственное решение нашего сравнения.

Т е о р е м а 12. *Если* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *— каноническое разложение модуля* m*, то сравнение*

$$f(x) \equiv 0 \pmod{m} \qquad (54)$$

равносильно системе сравнений:

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \dots \quad \dots \quad \dots \quad \dots\dots\dots \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}} \end{cases} \tag{55}$$

Доказательство. Решения системы (55) (определение 8) представляют собой классы по модулю m, равному наименьшему общему кратному чисел $p_1^{\alpha_1},\ p_2^{\alpha_2},\ \dots,\ p_k^{\alpha_k}$. Если класс $\overline{a}$ по модулю m удовлетворяет системе (55), т.е. если $f(a) \vdots p_1^{\alpha_1}, f(a) \vdots p_2^{\alpha_2},\ \dots,\ f(a) \vdots p_k^{\alpha_k}$, то согласно определению наименьшего общего кратного и его свойствам (см. «Алгебра», часть 1), $f(a) \vdots m \Leftrightarrow f(a) \equiv 0 \pmod{m}$, т.е. $\overline{a}$ представляет собой решение сравнения (54).

Наоборот, если класс $\overline{a}$ удовлетворяет сравнению (54), то $f(a) \vdots m$, а поскольку $m \vdots p_i^{\alpha_i}$, имеем: $f(a) \vdots p_i^{\alpha_i} \Leftrightarrow f(a) \equiv 0 \pmod{p_i^{\alpha_i}}$, при $i = 1,\ 2,\ \dots,\ k$, т.е. $\overline{a}$ — решение системы (55). Теорема доказана.

Задача 9. Решить сравнение:

$$x^2 - 2x - 1 \equiv 0 \pmod{18}.$$

Решение. Имеем: $m = 18 = 2 \cdot 3^3$. Тогда сравнение эквивалентно системе сравнений:

$$\begin{cases} x^2 - 2x - 1 \equiv 0 \pmod{2} \\ x^2 - 2x - 1 \equiv 0 \pmod{9}. \end{cases}$$

Для первого сравнения испытываем классы вычетов $\overline{0},\ \overline{1}$. Для второго сравнения аналогично испытываем классы вычетов $\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{7},\ \overline{8}$. Убеждаемся, что класс $\overline{1}$ удовлетворяет первому сравнению, но не удовлетворяет

второму, следовательно, система решений не имеет, тогда исходное сравнение (равносильное данной системе) тоже не будет иметь решений.

В теории сравнений большое значение имеет следующая теорема о максимальном числе решений сравнения:

Т е о р е м а 13. *Сравнение* (53) *имеет не более* n *решений.*

Д о к а з а т е л ь с т в о. Доказательство этой теоремы аналогично доказательству теоремы Безу в алгебре (см. «Алгебра», часть 1). Пусть сравнение (53) имеет решение x_1, т.е. $f(x_1) \equiv 0 \pmod{p}$. Тогда по теореме Безу имеем тождество:

$$f(x) = (x - x_1)f_1(x) + f(x_1),$$

где $f_1(x)$ — многочлен степени $n-1$ с неизменным старшим коэффициентом a_n, а $f(x_1) \vdots p$.

По модулю p это тождество переходит в тождественное сравнение

$$f(x) \equiv (x - x_1)f_1(x) \pmod{p}, \tag{56}$$

т.е. в сравнение, верное $\forall x \in \mathbb{Z}$, так что сравнение (53) эквивалентно сравнению

$$(x - x_1)f_1(x) \equiv 0 \pmod{p}.$$

Аналогично можем получить тождественное сравнение $f_1(x) \equiv (x - x_2)f_2(x) \pmod{p}$, если сравнение $f_1(x) \equiv 0 \pmod{p}$ имеет решение x_2 и т.д., пока не натолкнемся на неразрешимое сравнение $f_k(x) \equiv 0 \pmod{p}$ степени $n - k > 1$ или не дойдем до разрешимого сравнения первой степени $a_n(x - x_n) \equiv 0 \pmod{p}$.

Подстановкой по обратной цепочке получаем в первом случае тождественное сравнение

$$f(x) = (x - x_1)(x - x_2) \dots (x - x_k) f_k(x) \equiv 0 \pmod{p}, \quad (57)$$

которое показывает, что все найденные решения x_2, x_3, ... для $f_1(x) \equiv 0 \pmod{p}$, $f_2(x) \equiv 0 \pmod{p}$, ... являются также решениями сравнения (53). Других решений (53) иметь не может. Действительно, если $f(x_{k+1}) \equiv 0 \pmod{p}$ и $x_{k+1} \not\equiv x_1, x_2, \dots, x_k \pmod{p}$, то должно выполняться сравнение $f_k(x_{k+1}) \equiv 0 \pmod{p}$ (так как остальные множители не делятся на p), но это противоречит принятому условию о неразрешимости сравнения $f_k(x) \equiv 0 \pmod{p}$.

В случае n решений $x_1, x_2, \dots, x_n$ получается тождественное сравнение

$$f(x) = a_n(x - x_1)(x - x_2) \dots (x - x_n) \equiv 0 \pmod{p},$$

которое аналогичным образом свидетельствует о том, что (53) не может иметь более n решений. Теорема доказана.

2. Сравнения второй степени по простому модулю.

О п р е д е л е н и е 11. Сравнение вида

$$x^2 \equiv a \pmod{p} \quad (58)$$

называют *двучленным сравнением второй степени по простому модулю.*

Сравнение второй степени общего вида

$$Ax^2 + Bx + C \equiv 0 \pmod{M} \quad (59)$$

всегда можно привести к более простому двучленному сравнению. Это достигается следующим образом.

Умножим обе части и модуль сравнения (59) на $4A$; тогда имеем

$$4A^2x^2 + 4ABx + 4AC \equiv 0 \pmod{4AM} \Leftrightarrow$$

$$\Leftrightarrow 4A^2x^2 + 4ABx + B^2 - B^2 + 4AC \equiv 0 \pmod{4AM} \Leftrightarrow$$

$$\Leftrightarrow (2AX + B)^2 \equiv B^2 - 4AC \pmod{4AM}.$$

Обозначив здесь $2AX + B = y$, $B^2 - 4AC = D$, получаем двучленное сравнение

$$y^2 \equiv D \pmod{4AM}. \tag{60}$$

Ясно, что каждое число, удовлетворяющее (59), будет также удовлетворять (60), поэтому из неразрешимости (60) сразу же следует неразрешимость (59). Однако из разрешимости (60) относительно y еще не следует разрешимость (59) относительно x. В самом деле, каждое решение (60) $y \equiv y_1 \pmod{4AM}$ приводит нас к сравнению относительно x

$$2AX \equiv y_1 - B \pmod{4AM},$$

которое может оказаться неразрешимым, если $(y_1 - B) \not\vdots 2A$.

В случае разрешимости надо еще иметь в виду, что решения последнего сравнения получатся по модулю $2M$, в то время как мы должны указать решения по исходному модулю M сравнения (59). Переходя к модулю M, количество классов решений может уменьшиться.

Отметим в заключение, что при переходе от (59) к (60) в конкретной задаче не следует обязательно придерживаться общей схемы, а надо стараться упростить процесс выделения полного квадрата, для чего имеются различные возможности, однако мы на них останавливаться не станем.

Рассмотрим примеры приведения к двучленному сравнению.

Пример 1. $4x^2 - 11x - 3 \equiv 0 \pmod{13}$. Имеем:

$$4x^2-24x-16 \equiv 0 \pmod{13} \Leftrightarrow x^2-6x-4 \equiv 0 \pmod{13} \Leftrightarrow$$

$$\Leftrightarrow (x-3)^2-13 \equiv 0 \pmod{13} \Leftrightarrow (x-3)^2 \equiv 0 \pmod{13} \Leftrightarrow$$

$$\Leftrightarrow x \equiv 3 \pmod{13}.$$

Пример 2. $3x^2 + 7x + 8 \equiv 0 \pmod{17}$. Имеем:

$$3x^2+24x-9 \equiv 0 \pmod{17} \Leftrightarrow x^2+8x-3 \equiv 0 \pmod{17} \Leftrightarrow$$

$$\Leftrightarrow (x+4)^2 \equiv 19 \pmod{17} \Leftrightarrow (x+4)^2 \equiv 2 \pmod{17} \Leftrightarrow$$

$$\Leftrightarrow x+4 \equiv \pm 6 \pmod{17}.$$

Отсюда:

$$x+4 \equiv 6 \pmod{17} \Leftrightarrow x \equiv 2 \pmod{17};$$

$$x+4 \equiv -6 \pmod{17} \Leftrightarrow x \equiv -10 \equiv 7 \pmod{17}.$$

Определение 12. Если сравнение (58) разрешимо, то a называется *квадратичным вычетом по модулю* p; если же сравнение (58) не имеет решения, то a — *квадратичный невычет.*

Замечание. Случай, когда $p \vdots a$, является тривиальным, так как в этом и только в этом случае, очевидно, $x \equiv 0 \pmod{p}$. Поэтому исключим этот случай из дальнейшего рассмотрения и будем считать, что $(a,\ p) = 1$. Тогда решения сравнения (58) следует искать только среди классов вычетов приведенной системы по модулю p.

Процесс нахождения решения методом подбора является для сравнения (58) более простым, по сравнению с общим

случаем. Дело в том, что записывая приведенную систему вычетов по модулю p абсолютно наименьшими вычетами

$$\pm 1,\ \pm 2,\ \ldots,\ \pm\frac{p-1}{2},$$

мы можем пригодность их положительных и отрицательных значений проверять одновременно.

З а д а ч а 10. Определить, будет ли число $a = 3$ в сравнении $x^2 \equiv 3 \pmod 5$ квадратичным вычетом.

Р е ш е н и е. Запишем приведенную систему абсолютно наименьших вычетов по модулю 5: $\pm 1,\ \pm 2$. Тогда $(\pm 1)^2 \not\equiv \not\equiv 3 \pmod 5$ и $(\pm 2)^2 \not\equiv 3 \pmod 5$, следовательно, $a = 3$ — квадратичный невычет.

Т е о р е м а 14. *Если a — квадратичный вычет и p — нечетное простое число, то сравнение* (58) *имеет два решения.*

Д о к а з а т е л ь с т в о. Пусть a — квадратичный вычет и сравнение (58) имеет решение $x \equiv x_0 \pmod p$. Заметим, что $(-x_0)^2 \equiv a \pmod p$, т.е. $x \equiv -x_0 \pmod p$ — тоже решение сравнения. Покажем, что x_0 и $-x_0$ принадлежат различным классам. Действительно, если предположить, что $x_0 \equiv -x_0 \pmod p$, то получим: $2x_0 \equiv \equiv 0 \pmod p \Leftrightarrow 2x_0 \vdots p$. Так как $(2,\ p) = 1$, то $x_0 \vdots p$. Однако этого быть не может, так как x_0 выбран нами из приведенной системы вычетов по модулю p. Следовательно, $x_0 \not\equiv -x_0 \pmod p$, т.е. решения $x \equiv \equiv x_0 \pmod p$ и $x \equiv -x_0 \pmod p$ различны. Теорема доказана.

З а м е ч а н и е. По теореме о максимальном числе решений сравнения n-ой степени, сравнение (58) не может иметь более двух решений.

Т е о р е м а 15. *Если имеет место сравнение* (58), *где* p *— нечетное простое число, то среди приведенной системы вычетов по модулю* p *имеется точно* $\dfrac{p-1}{2}$ *квадратичных вычетов и столько же квадратичных невычетов.*

Д о к а з а т е л ь с т в о. Необходимо доказать, что существует точно $\dfrac{p-1}{2}$ значений a, при которых сравнение (58) будет иметь решение и столько же различных значений a, при которых это сравнение не будет иметь решений.

Пусть $\pm 1,\ \pm 2,\ \ldots,\ \pm\dfrac{p-1}{2}$ — приведенная система абсолютно наименьших вычетов по модулю p. Будем подставлять все эти вычеты в сравнение (58) вместо x. При этом в левой части получаются числа

$$1^2,\ 2^2,\ 3^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2. \tag{61}$$

В случае сравнимости (по модулю p) одного из них, например k^2 с a (заметим, что больше чем в одном случае это, согласно предыдущему, быть не может), мы получаем решения

$$x \equiv \pm k \pmod{p}.$$

Одновременно видно, что по модулю p разрешимыми будут только такие сравнения (58), в которых a сравнимо по модулю p с числами ряда (61). Другими словами, в ряде (61) записаны все квадратичные вычеты по модулю p. Все они принадлежат различным классам. Действительно, если предположить противное, т.е. что для

$$1 \leqslant k < l \leqslant \frac{p-1}{2}$$

имеет место сравнение

$$k^2 \equiv l^2 \pmod{p},$$

то оказалось бы, что (в силу транзитивности отношения сравнимости) сравнение (58) имеет 4 решения

$$x \equiv \pm k \pmod{p} \text{ и } x \equiv \pm l \pmod{p},$$

что противоречит теореме о максимальном числе решений сравнения n-ой степени по модулю p. Следовательно, все $\dfrac{p-1}{2}$ квадратичных вычетов принадлежат различным классам по модулю p. Так как в приведенной системе вычетов по модулю p содержится ровно $p-1$ чисел, то понятно, что количество квадратичных невычетов будет равно разности $(p-1) - \left(\dfrac{p-1}{2}\right) = \dfrac{p-1}{2}$. Теорема доказана.

З а д а ч а 11. Найти все квадратичные вычеты и вычеты по модулю 13.

Р е ш е н и е. Записываем приведенную систему абсолютно наименьших вычетов по модулю 13:

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 5,\ \pm 6.$$

Тогда сравнения

$$\begin{aligned}
x^2 &\equiv 1 \pmod{13} \\
x^2 &\equiv 4 \pmod{13} \\
x^2 &\equiv 9 \pmod{13} \\
x^2 &\equiv 16 \pmod{13} \\
x^2 &\equiv 25 \pmod{13} \\
x^2 &\equiv 36 \pmod{13}
\end{aligned}$$

будут иметь решения. Заменим эти сравнения эквивалент-

ными:

$$\begin{aligned} x^2 &\equiv 1 \pmod{13} \\ x^2 &\equiv 4 \pmod{13} \\ x^2 &\equiv 9 \pmod{13} \\ x^2 &\equiv 3 \pmod{13} \\ x^2 &\equiv 12 \pmod{13} \\ x^2 &\equiv 10 \pmod{13}. \end{aligned}$$

Видно, что $1,\ 3,\ 4,\ 9,\ 10,\ 12$ — квадратичные вычеты. Сравнения

$$\begin{aligned} x^2 &\equiv 2 \pmod{13} \\ x^2 &\equiv 5 \pmod{13} \\ x^2 &\equiv 6 \pmod{13} \\ x^2 &\equiv 7 \pmod{13} \\ x^2 &\equiv 8 \pmod{13} \\ x^2 &\equiv 11 \pmod{13} \end{aligned}$$

решений не имеют, т.е. $2,\ 5,\ 6,\ 7,\ 8,\ 11$ — квадратичные невычеты.

Следующая теорема позволяет определять, будет ли a квадратичным вычетом или невычетом, не решая сравнения (58).

Т е о р е м а 16 (к р и т е р и й Э й л е р а). *Число a, которое не делится на нечетное простое p, является квадратичным вычетом по модулю p тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, и квадратичным невычетом тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Д о к а з а т е л ь с т в о. По теореме Ферма имеем для $(a,\ p) = 1$ и $(2,\ p) = 1$

$$a^{p-1} \equiv 1 \pmod{p},$$

или

$$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \pmod{p},$$

или

$$\left(a^{\frac{p-1}{2}}+1\right)\left(a^{\frac{p-1}{2}}-1\right)\vdots p.$$

Отсюда видно, что, по крайней мере, одна из скобок должна делиться на p. Но обе скобки не могут делиться на p, так как в этом случае на p делилась бы и их разность 2, что невозможно, ибо $(2,\ p)=1$.

Если a является квадратичным вычетом, то

$$\left(a^{\frac{p-1}{2}}-1\right)\vdots p,\ \text{т.е. } a^{\frac{p-1}{2}}\equiv 1 \pmod p. \tag{62}$$

Действительно, в этом случае существует такое значение $x\in\mathbb{Z},\ (x,\ p)=1$, что

$$a\equiv x^2 \pmod p,$$

откуда

$$a^{\frac{p-1}{2}}\equiv\left(x^2\right)^{\frac{p-1}{2}}\equiv x^{p-1}\equiv 1 \pmod p.$$

Так как по модулю p имеется $\dfrac{p-1}{2}$ квадратичных вычетов, то полученный результат означает, что сравнение (62) имеет не менее $\dfrac{p-1}{2}$ решений, если будем в нем a рассматривать как неизвестное. Но сравнение (62), как сравнение по простому модулю, не может иметь большее число решений, чем степень сравнения, т.е. больше чем $\dfrac{p-1}{2}$.

Итак, для всех квадратичных вычетов и только для них выполняется (62). Но тогда для остальных a, $(a,\ p)=1$, т.е. для квадратичных невычетов и только для них

$$\left(a^{\frac{p-1}{2}}+1\right)\vdots p \text{ или } a^{\frac{p-1}{2}}\equiv -1 \pmod p.$$

Критерий Эйлера доказан.

З а д а ч а 12. Выяснить, будет ли число 3 квадратичным вычетом или невычетом по модулю 7.

Р е ш е н и е. Имеем:

$$3^{\frac{7-1}{2}} \equiv 27 \pmod 7 \Leftrightarrow 3^{\frac{7-1}{2}} \equiv -1 \pmod 7,$$

следовательно, 3 — есть квадратичный невычет.

Глава VI. Степенные вычеты

§1. Показатели и их основные свойства.

1. Мультипликативная группа обратимых элементов в кольце вычетов. Пусть дано коммутативно-ассоциативное кольцо с единицей $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$. Из курса алгебры мы знаем, что $\langle \mathbb{Z}_m,\ \oplus \rangle$ — циклическая и периодическая абелева группа, а также, что $\langle \mathbb{Z}_m,\ \odot \rangle$ — полугруппа (см. «Алгебра», часть 3). Обозначим через M множество обратимых элементов кольца $\mathbb{Z}_m$ и покажем, что алгебра $\langle M,\ \odot \rangle$ будет конечной абелевой группой порядка $\varphi(m)$.

Докажем сначала следующую теорему об обратимых элементах любого кольца.

Т е о р е м а 1. *Множество $\widetilde{R}$ обратимых элементов коммутативно-ассоциативного кольца R с единицей образует абелеву группу относительно операции умножения.*

Д о к а з а т е л ь с т в о. Так как по условию кольцо R коммутативно, ассоциативно и обладает единицей, то для доказательства теоремы достаточно показать справедливость двух утверждений:

а) произведение двух обратимых элементов обратимо в R;

б) если ε — обратимый элемент, то и ε^{-1} обратимо в R.

Пусть δ и ε обратимы в R. Тогда $\exists \delta_1,\ \varepsilon_1 \in R:\ (\delta\delta_1 = e)\ \&\ (\varepsilon\varepsilon_1 = e)$. Но тогда имеем: $(\delta\varepsilon)(\delta_1\varepsilon_1) = (\varepsilon\delta)(\delta_1\varepsilon_1) = \varepsilon(\delta\delta_1)\varepsilon_1 = \varepsilon e\varepsilon_1 = \varepsilon\varepsilon_1 = e$. Значит, $\delta\varepsilon$ тоже обратимо в R. Этим доказано утверждение а). Утверждение б) сразу следует из того, что если $\varepsilon\varepsilon_1 = e$, то не только ε, но и $\varepsilon_1 = \varepsilon^{-1}$ обратимо в R.

Единичным элементом группы $\widetilde{R}$ является, очевидно,

единица e кольца R. Теорема доказана.

Описание обратимых элементов в кольце вычетов $\mathbb{Z}_m$ дается следующей теоремой:

Т е о р е м а 2. *Для того, чтобы класс вычетов $\overline{k}$ по модулю m был обратимым, необходимо и достаточно, чтобы $\overline{k}$ и m были взаимно просты.*

Д о к а з а т е л ь с т в о.

Н е о б х о д и м о с т ь. Пусть $\overline{k}$ — класс вычетов по модулю m, являющийся обратимым в $\mathbb{Z}_m$. Тогда существует такой класс вычетов $\overline{x}$ по модулю m, что $\overline{k} \odot \overline{x} = \overline{1}$. Выберем в $\overline{k}$ элемент k, а в $\overline{x}$ элемент x. Тогда $kx \equiv 1 \pmod{m}$, т.е. $(kx-1) \vdots m$, или $kx-1 = my$, $y \in \mathbb{Z}$. Из этого равенства следует, что наибольший общий делитель k и m равен 1, т.е. что $(k,\ m) = 1$. Тогда, согласно следствию свойства 8 сравнений (п.2 §1 гл. IV) $\overline{k}$ и m взаимно просты.

Д о с т а т о ч н о с т ь. Пусть класс вычетов $\overline{k}$ взаимно прост с m. Выберем в $\overline{k}$ число k. Так как по условию $(k,\ m) = 1$, то найдутся такие целые числа x и y, что $kx+my = 1$ (см. «Алгебра», часть 1). Но тогда $kx-1 = -my$ делится на m, и поэтому $kx \equiv 1 \pmod{m}$. Из этого равенства следует, что $\overline{k} \odot \overline{x} = \overline{1}$, где $\overline{x}$ — класс вычетов, содержащий x. Это и значит, что $\overline{k}$ — обратимый элемент в $\mathbb{Z}_m$. Теорема доказана.

Из теоремы следует, что множество M обратимых элементов в $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$ совпадает с множеством классов вычетов по модулю m, взаимно простых с m. Так как количество таких классов равно $\varphi(m)$, то алгебра $\langle M,\ \odot \rangle$ является конечной абелевой группой порядка $\varphi(m)$. Ее называют *мультипликативной группой обратимых элементов в* $\langle \mathbb{Z}_m,\ \oplus,\ \odot \rangle$.

2. Порядок класса вычетов. Все элементы группы $\langle M,\ \odot\rangle$ (т.е. все классы вычетов по модулю m, взаимно простые с m) имеют конечный порядок и этот порядок является делителем $\varphi(m)$ (числа элементов группы M). Это вытекает из следствия 1 теоремы Лагранжа (см. «Алгебра», часть 3).

Учитывая определение порядка элемента k в группе M, дадим следующее определение порядка класса вычетов по модулю m.

О п р е д е л е н и е 1. *Порядком класса вычетов* $\overline{k}$, взаимно простого с модулем m, называют наименьшее натуральное число δ, такое, что $\overline{k^\delta} = \overline{1}$.

Число δ называют также порядком всех чисел k, входящих в класс вычетов $\overline{k}$. Если $k \in \overline{k}$, то из равенства $\overline{k^\delta} = \overline{1}$ следует, что $k^\delta \equiv 1 \pmod m$.

Таким образом, можно дать другое определение:

О п р е д е л е н и е 2. Пусть $(k,\ m) = 1$. *Порядком числа* k *по модулю* m называют наименьшее натуральное число δ, такое, что $k^\delta \equiv 1 \pmod m$.

Если порядок класса вычетов $\overline{k}$ (соответственно, числа k) по модулю m равен δ, то говорят, что δ является показателем класса $\overline{k}$ (соответственно, числа k) по модулю m, или что класс $\overline{k}$ (соответственно, число k) принадлежит показателю δ по модулю m. Пишут: $\overline{k} \in \delta$.

З а м е ч а н и е. Если порядок класса вычетов $\overline{k}$ по модулю m равен δ, то циклическая подгруппа G_k, порожденная классом вычетов $\overline{k}$ в группе M, состоит из δ элементов: $|G_k| = \delta$. Порядок δ подгруппы G_k в силу теоремы Лагранжа будет делителем $\varphi(m)$ и будет совпадать с порядком образующего элемента (класса) этой подгруппы, поэтому

имеет место равенство: $|G_k| = p(\overline{k}) = \delta$.

Покажем, что для циклической группы M и ее подгрупп (которые тоже будут циклическими) справедливы все теоремы, доказанные для циклических групп в курсе алгебры (см. «Алгебра», часть 3).

Т е о р е м а 3. *Если порядок класса вычетов k по модулю m равен δ, то сравнение $k^\gamma \equiv 1 \pmod m$ выполняется в том и только в том случае, когда $\gamma \vdots \delta$.*

Д о к а з а т е л ь с т в о.

Н е о б х о д и м о с т ь. Пусть $\overline{k} \in \delta \Rightarrow k^\delta \equiv 1 \pmod m$. Разделим γ на δ с остатком: $\gamma = \delta t + r$, где $0 \leqslant r < \delta$. Так как $k^\gamma \equiv 1 \pmod m$, то $(k^\delta)^t \cdot k^r \equiv 1 \pmod m \Rightarrow k^r \equiv 1 \pmod m$. Поскольку $r < \delta$, получаем противоречие с условием: $\overline{k} \in \delta$. Следовательно, γ делится на δ без остатка.

Д о с т а т о ч н о с т ь. Пусть $\overline{k} \in \delta$ и $\gamma \vdots \delta$. Докажем, что $k^\gamma \equiv 1 \pmod m$. Так как $\overline{k} \in \delta$, то $k^\delta \equiv 1 \pmod m$, Но $\gamma = \delta t$, $t \in \mathbb{Z}$, поэтому $k^\gamma = k^{\delta t} = (k^\delta)^t \equiv 1 \pmod m$. Теорема доказана.

С л е д с т в и е. *Если порядок класса вычетов k по модулю m равен δ, то $\varphi(m) \vdots \delta$.*

Д о к а з а т е л ь с т в о. Поскольку $(k,\ m) = 1$, то по теореме Эйлера $k^{\varphi(m)} \equiv 1 \pmod m$, а так как $\overline{k} \in \delta$, то $k^\delta \equiv 1 \pmod m$. Тогда по теореме 3 $\varphi(m) \vdots \delta$, т.е. мы еще раз доказали, что показателями могут быть только делители $\varphi(m)$. Следствие доказано.

Т е о р е м а 3. *Если порядок класса вычетов k по модулю m равен δ, то сравнение $k^{\gamma_1} \equiv k^{\gamma_2} \pmod m$ выполняется в том и только в том случае, когда разность $\gamma_1 - \gamma_2$ делится на δ.*

Д о к а з а т е л ь с т в о.

Н е о б х о д и м о с т ь. Имеем: $k^{\delta} \equiv 1 \pmod{m}$ и $k^{\gamma_1} \equiv k^{\gamma_2} \pmod{m}$. Если $\gamma_1 > \gamma_2$, то $k^{\gamma_1-\gamma_2} \equiv 1 \pmod{m} \Rightarrow$ $\Rightarrow (\gamma_1 - \gamma_2) \vdots \delta$. Воспользовавшись свойством симметричности отношения сравнимости, можно аналогично рассмотреть случай, когда $\gamma_1 < \gamma_2$.

Д о с т а т о ч н о с т ь. Если $k^{\delta} \equiv 1 \pmod{m}$ и $(\gamma_1 - \gamma_2) \vdots \delta$, то $\gamma_1 - \gamma_2 = \delta t$, где $t \in \mathbb{Z}$. Тогда $k^{\delta t} = (k^{\delta})^t =$ $= k^{\gamma_1-\gamma_1} \equiv 1 \pmod{m} \Rightarrow k^{\gamma_1} \equiv k^{\gamma_2} \pmod{m}$. Теорема доказана.

З а м е ч а н и е. Из теоремы следует, что показатели сравниваются по модулю δ, где δ — порядок класса вычетов $\overline{k}$ по модулю m.

Т е о р е м а 4. *Если порядок класса вычетов $\overline{k}$ по модулю m равен δ, то в ряду степеней k^0, k^1, k^2, $\ldots$, $k^{\delta-1}$ нет сравнимых между собой чисел по модулю m.*

Д о к а з а т е л ь с т в о. Предположим противное, т.е. пусть $k^p \equiv k^q \pmod{m}$, где $0 \leqslant q < p \leqslant \delta - 1$. Тогда из условия, что $(k,\ m) = 1$ получаем $k^{p-q} \equiv 1 \pmod{m}$, $0 < p - q < \delta$, но это невозможно, так как k принадлежат показателю δ по модулю m. Следовательно, $k^p \not\equiv$ $\not\equiv k^q \pmod{m}$. Теорема доказана.

З а д а ч а 1. Найти показатель, которому принадлежит число 3 по модулю 7.

Р е ш е н и е. Из доказанных выше теорем следует, что показателем числа 3 (класса $\overline{3}$) могут быть только натуральные делители числа $\varphi(7) = 6$. Ими являются числа 1, 2, 3, 6. Тогда:

$$3^1 \equiv 3 \pmod{7} \qquad 3^2 \equiv 2 \pmod{7}$$
$$3^3 \equiv -1 \pmod{7} \qquad 3^6 \equiv 1 \pmod{7}.$$

Последнее сравнение свидетельствует о том, что показатель класса $\overline{3}$ (соответственно, числа 3) по модулю 6 равен 6. Другими словами, $\overline{3} \in 6$.

З а д а ч а 2. Существуют ли еще классы вычетов по модулю 7, которые принадлежат показателю $\delta = 6$ и сколько их?

Р е ш е н и е. Мы должны решить сравнение $x^6 \equiv \equiv 1 \pmod 7$. Одно решение этого сравнения мы уже знаем из задачи 1: $x \equiv 3 \pmod 7$. Чтобы найти остальные решения, запишем приведенную систему вычетов по модулю 7: 1, 2, 3, 5, 6 и все возможные показатели по модулю 7: 1, 2, 3, 6. Тогда:

$$
\begin{array}{lll}
1^1 \equiv 1 \pmod 7 & & 4^1 \equiv 4 \pmod 7 \\
2^1 \equiv 2 \pmod 7 & & 4^2 \equiv 2 \pmod 7 \\
2^2 \equiv 4 \pmod 7 & & 4^3 \equiv 1 \pmod 7 \\
2^3 \equiv 1 \pmod 7 & & 5^1 \equiv 5 \pmod 7 \\
3^1 \equiv 3 \pmod 7 & & 5^2 \equiv 4 \pmod 7 \\
3^2 \equiv 4 \pmod 7 & & 5^3 \equiv -1 \pmod 7 \\
3^3 \equiv -1 \pmod 7 & & 5^6 \equiv 1 \pmod 7 \\
3^6 \equiv 1 \pmod 7 & & 6^1 \equiv -1 \pmod 7 \\
 & & 6^2 \equiv 1 \pmod 7.
\end{array}
$$

Итак, порядок (показатель) $\delta = 6$ имеют классы $\overline{3}$ и $\overline{5}$, т.е. показателю $\delta = 6$ принадлежат два класса вычетов.

З а м е ч а н и е. В процессе решения данной задачи нам пришлось все числа приведенной системы вычетов по модулю 7 распределять по всем показателям по модулю 7, поскольку, например, класс вычетов 6 удовлетворяет сравнению $x^6 \equiv 1 \pmod 7$, но он уже принадлежит показателю $\delta = 2$, так как $6^2 \equiv 1 \pmod 7$, и не может принадлежать показателю $\delta = 6$.

Ответ на вопрос, сколько классов вычетов принадлежат данному показателю по простому модулю, дадим в следующем пункте.

3. Число классов вычетов, принадлежащих данному показателю по модулю m.

Т е о р е м а 5. *Если по простому модулю p существует хотя бы один класс вычетов, принадлежащий показателю δ, то таких классов будет ровно $\varphi(\delta)$.*

Д о к а з а т е л ь с т в о. Так как по условию p — простое число, то $\varphi(p) = p - 1$ и δ является делителем $(p-1)$. Предположим, что существует число $k \in \delta$, т.е. $k^\delta \equiv 1 \pmod p$. Наша задача — найти все $x \in \delta$, т.е. решить сравнение $x^\delta \equiv 1 \pmod p$. Все эти решения находятся в приведенной системе вычетов по модулю p: $1,\ 2,\ 3,\ \ldots,\ p-1$. Покажем, что вместо этой системы можно использовать систему:

$$k^0,\ k^1,\ k^2,\ \ldots,\ k^s,\ \ldots,\ k^{\delta-1}. \tag{63}$$

Действительно:

а) все числа этой системы попарно несравнимы по модулю p (теорема 4);

б) все числа удовлетворяют сравнению $x^\delta \equiv 1 \pmod p$, так как $(k^s)^\delta = (k^\delta)^s \equiv 1 \pmod p$;

в) количество чисел в последовательности (63) равно δ, т.е. максимально возможному количеству решений сравнения $x^\delta \equiv 1 \pmod p$.

Остается выбрать из последовательности чисел (63) те, которые принадлежат показателю δ по модулю p. Выясним, какому условию должны удовлетворять показатели степеней в ряду (63), чтобы $k^i \in \delta$.

Пусть $(i,\ \delta) = 1$ и $k^i \in \gamma$, тогда $(k^i)^\gamma \equiv 1 \pmod p$. Так

как по условию теоремы $k^{\delta} \equiv 1 \pmod{p}$, то $i\gamma \vdots \delta$. Поскольку $(i,\ \delta) = 1$, будем иметь $\gamma \vdots \delta \Leftrightarrow \gamma = \delta t$, где $t \in \mathbb{Z}$. Тогда наименьшее положительное значение, которое может принимать γ, будет равно δ (при $t = 1$), т.е. имеем: $\gamma = \delta$.

Если же $(i,\ \delta) = d > 1$, то из того, что $i\gamma \vdots \delta$ будет следовать: $i\gamma = \delta t$, где $t \in \mathbb{Z}$. Положив $t = 1$, получим, что $i\gamma = \delta$ и наименьшее натуральное значение γ будет меньше δ, т.е. $k^i \in \gamma$, где $\gamma < \delta$. Следовательно, в последовательности (63) порядку (показателю) δ будут принадлежать все те k^i, для которых выполняется условие $(i,\ \delta) = 1$. Таких чисел будет ровно $\varphi(\delta)$, так как числа $0,\ 1,\ 2,\ \ldots,\ \delta - 1$ представляют полную систему вычетов по модулю δ. Теорема доказана.

З а д а ч а 3. Найти все классы вычетов, принадлежащие показателю $\delta = 6$ по модулю 13.

Р е ш е н и е. Сначала найдем одно из чисел, принадлежащих показателю $\delta = 6$ по модулю 13. Для этого запишем приведенную систему вычетов по модулю 13:

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12.$$

Показатели по модулю 13 — это делители числа 12:

$$1,\ 2,\ 3,\ 4,\ 6,\ 12.$$

Будем возводить числа $1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12$ в степени $1,\ 2,\ 3,\ 4,\ 6,\ 12$ до тех пор, пока не получим число, сравнимое с 1 по модулю 13:

$$\begin{array}{llll} 1^1 \equiv 1 & \pmod{13} & 3^1 \equiv 3 & \pmod{13} \\ 2^1 \equiv 2 & \pmod{13} & 3^2 \equiv 9 & \pmod{13} \\ 2^2 \equiv 4 & \pmod{13} & 3^3 \equiv 1 & \pmod{13} \\ 2^3 \equiv 8 & \pmod{13} & 4^1 \equiv 4 & \pmod{13} \\ 2^4 \equiv 3 & \pmod{13} & 4^2 \equiv 3 & \pmod{13} \end{array}$$

$$2^6 \equiv -1 \pmod{13} \qquad 4^3 \equiv -1 \pmod{13}$$
$$2^{12} \equiv 1 \pmod{13} \qquad 4^4 \equiv 9 \pmod{13}$$
$$4^6 \equiv 1 \pmod{13}.$$

Имеем: $\overline{1} \in 1$, $\overline{2} \in 12$, $\overline{3} \in 3$, $\overline{4} \in 6$. Чтобы найти остальные классы вычетов по модулю 13, имеющие порядок 6, составим последовательность

$$4^0,\ 4^1,\ 4^2,\ 4^3,\ 4^4,\ 4^5,$$

из которой выбираем те члены, показатели степеней у которых взаимно просты с $\delta = 6$, т.е. числа 4^1 и 4^5. Значит, искомыми классами вычетов являются $\overline{4^1}$ и $\overline{4^5}$. Но $4^5 \equiv 4^2 \cdot 4^2 \cdot 4 \equiv 3 \cdot 3 \cdot 4 \equiv 36 \equiv 10 \pmod{13}$ и потому получаем классы $\overline{4}$ и $\overline{10}$. Таким образом, показателю $\delta = 6$ принадлежат два класса вычетов по модулю 13: $\overline{4}$ и $\overline{10}$. Этот факт подтверждает также и то, что $\varphi(6) = 2$.

4. Первообразные корни по простому модулю.

О п р е д е л е н и е 3. *Первообразным корнем по простому модулю* p называют класс вычетов $\overline{k}$ по этому модулю, порядок которого равен $p - 1$.

З а м е ч а н и е. Из определения следует, что если $\overline{k}$ — первообразный корень, то $\overline{k^{p-1}} = \overline{1}$ или $k^{p-1} \equiv 1 \pmod{p}$.

Из теорем 3 и 4 получаем свойства первообразных корней:

С в о й с т в о 1. *Если* $\overline{k}$ *— первообразный корень по простому модулю* p, *то* $\overline{k^{\gamma_1}} = \overline{k^{\gamma_2}}$ *в том и только в том случае, когда* $\gamma_1 - \gamma_2$ *делится на* $p - 1$.

С в о й с т в о 2. *Если* $\overline{k}$ *— первообразный корень по простому модулю* p, *то в ряду степеней*

$$\overline{1},\ \overline{k},\ \overline{k^2},\ \ldots,\ \overline{k^{p-2}}$$

все члены различны (в этом случае $\delta = p - 1$).

Но этот ряд степеней содержит $p-1$ элемент, т.е. столько же элементов, сколько их в приведенной системе вычетов по модулю p (или, что то же самое, в группе $\langle M,\ \odot\rangle$ обратимых элементов кольца $\langle \mathbb{Z}_m,\ \oplus,\ \odot\rangle$). Так как все степени $\overline{k}$ взаимно просты с $\overline{p}$ (т.е. обратимы), то получим следующий важный результат:

Если $\overline{k}$ — первообразный корень по простому модулю p, то множество классов вычетов $\overline{1},\ \overline{k},\ \overline{k^2},\ \ldots,\ \overline{k^{p-2}}$ совпадает с множеством классов вычетов, взаимно простых с p:

$$\left\{\overline{1},\ \overline{k},\ \overline{k^2},\ \ldots,\ \overline{k^{p-2}}\right\} = \left\{\overline{1},\ \overline{2},\ \overline{3},\ \ldots,\ \overline{p-1}\right\}.$$

Полученный результат можно сформулировать следующим образом:

Т е о р е м а 6. *Если $\overline{k}$ — первообразный корень по простому модулю p, то для любого ненулевого класса вычетов $\overline{x}$ по модулю p найдется одно и только одно число γ, такое, что $\overline{x} = \overline{k^\gamma}$ и $0 \leqslant \gamma \leqslant p-2$.*

Из теоремы 5 вытекает, что если существует хотя бы один первообразный корень $\overline{k}$ по простому модулю p, то общее число таких корней равно $\varphi(p-1)$. Это будут классы вычетов вида $\overline{k^\gamma}$, где γ взаимно просто с $p-1$ и $0 \leqslant \gamma \leqslant p-2$.

Покажем теперь, что условие существования хотя бы одного первообразного корня излишне: такой корень существует для любого простого модуля $p > 2$. Это утверждение вытекает из следующей теоремы:

Т е о р е м а 7. *Пусть $p > 2$ — простое число и $(p-1) \vdots \delta$. Тогда количество классов вычетов по модулю p, имеющих порядок δ, равно $\varphi(\delta)$.*

Д о к а з а т е л ь с т в о. По следствию 1 теоремы Лагранжа (см. «Алгебра», часть 3) порядок любого из класса вычетов $\overline{1},\ \overline{2},\ \ldots,\ \overline{p-1}$ является делителем

$\varphi(p) = p - 1$. Обозначим через $\psi(\delta)$ число классов вычетов по модулю p, имеющих порядок δ. По теореме 5 получаем, что если есть хотя бы один класс вычетов порядка δ, то их число равно $\varphi(\delta)$. Таким образом, $\psi(\delta) = \varphi(\delta)$, если есть хотя бы один класс вычетов по модулю p порядка δ и $\psi(\delta) = 0$, если нет ни одного класса вычетов по модулю p порядка δ. Поэтому для любого делителя δ числа $p - 1$ выполняется неравенство $\psi(\delta) \leqslant \varphi(\delta)$. Обозначим делители числа $p - 1$ через $\delta_1, \delta_2, \ldots, \delta_k$. Так как порядок любого из классов вычетов $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ является одним из делителей числа $p - 1$, т.е. одним из чисел δ_j, $1 \leqslant j \leqslant k$, то

$$\psi(\delta_1) + \psi(\delta_2) + \ldots + \psi(\delta_k) = p - 1.$$

С другой стороны, по тождеству Гаусса (см. п.2 §3 гл. IV) имеем:

$$\varphi(\delta_1) + \varphi(\delta_2) + \ldots + \varphi(\delta_k) = p - 1.$$

Из последних двух равенств вытекает, что

$$\psi(\delta_1) + \psi(\delta_2) + \ldots + \psi(\delta_k) = \varphi(\delta_1) + \varphi(\delta_2) + \ldots + \varphi(\delta_k). \quad (64)$$

Но для любого j, $1 \leqslant j \leqslant k$, выполняется неравенство $\psi(\delta) \leqslant \varphi(\delta)$. Поэтому равенство (64) может иметь место лишь при условии, что $\forall j \ \psi(\delta_j) = \varphi(\delta_j)$. А это и означает, что количество классов вычетов по модулю p, имеющих порядок δ_j, равно $\varphi(\delta_j)$. Теорема доказана.

Применяя эту теорему к случаю $\delta = p - 1$, получаем важное следствие.

С л е д с т в и е. *Если $p > 2$ — простое число, то существует в точности $\varphi(p - 1)$ первообразных корней по модулю p.*

З а д а ч а 4. Найти все первообразные корни по модулю 13.

Р е ш е н и е. Записываем приведенную систему вычетов по модулю 13:

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12.$$

Далее выпишем все делители числа $13-1=12$:

$$1,\ 2,\ 3,\ 4,\ 6,\ 12.$$

Теперь находим первый первообразный корень, т.е. решаем сравнение $x^{12}\equiv 1 \pmod{13}$. В процессе решения задачи 3 мы его нашли: $2^{12}\equiv 1 \pmod{13}$. Записываем систему

$$2^0,\ 2^1, 2^3,\ 2^4, 2^5,\ 2^6, 2^7,\ 2^8, 2^9,\ 2^{10},\ 2^{11},$$

члены которой имеют показатели степеней, образующие полную систему вычетов по модулю 12. Выбираем из этой последовательности те члены, показатели степеней у которых взаимно просты с числом 12: $2^1,\ 2^5,\ 2^7,\ 2^{11}$. Первообразными корнями будут классы: $\overline{2}$, $\overline{2^5}=\overline{6}$, $\overline{2^7}=\overline{11}$, $\overline{2^{11}}=\overline{7}$.

Проверим, что мы правильно определили количество классов вычетов, принадлежащих показателю $\delta=12$, т.е. количество первообразных корней по модулю 13. Для этого вычисляем $\varphi(12)=\varphi(2^2\cdot 3)=12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=12\cdot\frac{1}{2}\cdot\frac{2}{3}=$ $=4$.

Итак, первообразными корнями по модулю 13 являются классы вычетов $\overline{2},\ \overline{6},\ \overline{7},\ \overline{11}$.

З а м е ч а н и е. До сих пор еще не найден эффективный способ нахождения хотя бы одного первообразного корня по данному модулю. На практике обычно используют метод испытаний. Если же найден один первообразный корень $\overline{k}$, то, как мы уже установили выше, остальные находятся легко.

§2. Индексы

1. Индексы по простому модулю. Общеизвестно, какое большое значение в разных разделах математики и в особенности в вычислительной практике имеют логарифмы. В теории чисел вводится сходный с логарифмами аппарат, который мы будем называть индексами. Логарифмом x по основанию k, как известно, называется показатель степени, в которую надо возвести число k, чтобы получить число x. В теории чисел аналогично этому рассматривают показатель степени k, сравнимой с x по рассматриваемому модулю m, и такой показатель называют индексом x по модулю m и основанию k.

Ранее мы показали, что если $\overline{k}$ — первообразный корень по простому модулю p, то для любого оличного от нуля класса вычетов $\overline{x}$ по модулю p найдется такое число γ, что $\overline{k^\gamma} = \overline{x}$.

О п р е д е л е н и е 1. Пусть p — простое число и $\overline{k}$ — первообразный корень по модулю p. Число γ называется *индексом класса вычетов* $\overline{x}$ *по модулю* p *при основании* $\overline{k}$, если $\overline{k^\gamma} = \overline{x}$. Записывают: $\operatorname{ind}_{\overline{k}} \overline{x} = \gamma$; читают: «индекс класса вычетов $\overline{x}$ по простому модулю p при первообразном корне $\overline{k}$ равен γ».

Разумеется, формулируя определение 1, можно говорить не о классах вычетов, а о самих вычетах. Число γ называют первообразным корнем по простому модулю p, если его порядок по этому модулю равен $p-1$. *Индексом числа* x *по модулю* p *при первообразном корне* $\overline{k}$, называют такое число γ, что

$$k^\gamma \equiv x \pmod{p},$$

где $0 \leqslant \gamma \leqslant p-2$. Это сравнение задает биекцию

$$\sigma : \left\{\overline{1},\ \overline{k},\ \overline{k^2},\ \ldots,\ \overline{k^{p-2}}\right\} \to \left\{\overline{1},\ \overline{2},\ \overline{3},\ \ldots,\ \overline{p-1}\right\}.$$

Из свойств первообразных корней следует, что $\overline{k^{\gamma_1}} = \overline{k^{\gamma_2}}$ в том и только в том случае, когда $\gamma_1 \equiv \gamma_2 \pmod{p-1}$. Поэтому, если γ — индекс числа x по простому модулю p при первообразном корне k, то и все числа γ', сравнимые с γ по модулю $p-1$, являются индексами x по модулю p при первообразном корне k.

Основные свойства индексов таковы:

С в о й с т в о 1. *Индекс произведения сравним по модулю $p-1$ с суммой индексов сомножителей.*

$$\operatorname{ind}_{\overline{k}} \overline{n_1} + \operatorname{ind}_{\overline{k}} \overline{n_2} \equiv \operatorname{ind}_{\overline{k}} \overline{n_1} \odot \overline{n_2} \pmod{p-1}. \qquad (65)$$

Д о к а з а т е л ь с т в о. По определению индексов имеем:

$$\overline{k}^{\operatorname{ind}_{\overline{k}} \overline{n_1}} = \overline{n_1}\,, \quad \overline{k}^{\operatorname{ind}_{\overline{k}} \overline{n_2}} = \overline{n_2}\,.$$

Перемножая эти равенства, получим:

$$\overline{k}^{\operatorname{ind}_{\overline{k}} \overline{n_1} + \operatorname{ind}_{\overline{k}} \overline{n_2}} = \overline{k}^{\operatorname{ind}_{\overline{k}} \overline{n_1} \odot \overline{n_2}}\,.$$

Отсюда и следует сравнение (65). Свойство доказано.

С л е д с т в и е. *Индекс степени (с натуральным показателем) сравним по модулю $p-1$ с произведением показателя степени на индекс основания степени:*

$$\operatorname{ind}_{\overline{k}} \left(\overline{n}\right)^s \equiv s \cdot \operatorname{ind}_{\overline{k}} \overline{n} \pmod{p-1}.$$

Обозначим через $\overline{\frac{n_1}{n_2}}$ класс вычетов $\overline{n_1} \odot \overline{n_2}^{-1}$.

Свойство 2. *Индекс дроби* $\overline{\frac{n_1}{n_2}}$ *сравним по модулю* $p-1$ *с разностью индексов числителя и знаменателя:*

$$\operatorname{ind}_{\overline{k}} \overline{\frac{n_1}{n_2}} \equiv \operatorname{ind}_{\overline{k}} \overline{n_1} - \operatorname{ind}_{\overline{k}} \overline{n_2} \pmod{p-1}. \tag{66}$$

Доказательство. Класс вычетов $\overline{x} = \overline{\frac{n_1}{n_2}}$ является решением уравнения $\overline{n_2} \odot \overline{x} = \overline{n_1}$. По свойству 1

$$\operatorname{ind}_{\overline{k}} \overline{n_1} \equiv \operatorname{ind}_{\overline{k}} \overline{n_2} + \operatorname{ind}_{\overline{k}} \overline{x} \pmod{p-1},$$

откуда и вытекает сравнение (66). Свойство доказано.

Свойство 3. *Индекс единицы сравним с нулем по модулю* $p-1$, *т.е.*

$$\operatorname{ind}_{\overline{k}} \overline{1} \equiv 0 \pmod{p-1},$$

так как $\overline{k}^0 = \overline{1}$.

Свойство 4. *Индекс основания индексов* $\overline{k}$ *сравним с единицей по модулю* $p-1$, *т.е.*

$$\operatorname{ind}_{\overline{k}} \overline{k} \equiv 1 \pmod{p-1},$$

так как $\overline{k}^1 = \overline{k}$.

Замечание.

а) Мы видим, что определение индексов и их свойства аналогичны определению и свойствам логарифмов.

б) Во всех случаях, когда речь идет о равенстве индексов, имеется в виду равенство их наименьших неотрицательных значений по модулю $p-1$.

в) В большинстве задач с применением индексов, так же как и в задачах с применением логарифмов, не важно, по

какому основанию $\overline{k}$ определяются индексы. Но если возникает необходимость перейти от индексов по основанию $\overline{k}$ к индексам по основанию $\overline{g}$, то применяется формула, аналогичная соответствующей формуле в теории логарифмов:

$$\operatorname{ind}_{\overline{g}} \overline{n} \equiv \operatorname{ind}_{\overline{k}} \overline{n} \cdot \operatorname{ind}_{\overline{g}} \overline{k} \pmod{p-1}.$$

2. Таблицы индексов. Составленные таблицы индексов для простых модулей p дают возможность по числу находить его индекс и, наоборот, по индексу — число. В качестве основания выбирается один из первообразных корней числа p.

Первые таблицы индексов для простых модулей до 200 составил в 1837 г. знаменитый русский математик Михаил Васильевич Остроградский (1801 – 1862), немецким математиком К. Якоби эти таблицы были доведены до 1000, а в настоящее время существуют таблицы индексов для простых модулей до 10000.

Таблицы обычно содержат наименьшие неотрицательные вычеты по модулю $\varphi(p) = p-1$ (первая таблица) и наименьшие неотрицательные приведенные вычеты чисел (вторая таблица). Эти таблицы помещаются в качестве приложения в конце каждого учебника по теории чисел. Покажем на примере составление таблиц по одному из модулей.

П р и м е р. Построить таблицы для определения индексов по числам и чисел по индексам по модулю $p = 7$.

В качестве основания $\overline{k}$ удобно взять наименьший первообразный корень по модулю 7. В задаче 2 (см. выше) мы нашли его: $\overline{k} = \overline{3}$. Запишем теперь две приведенных системы вычетов по модулю 7:

1) $1,\ 2,\ 3,\ 4,\ 5,\ 6$;

2) $3^0,\ 3^1,\ 3^2,\ 3^3,\ 3^4,\ 3^5$.

С помощью сравнений устанавливаем биективное соответствие между системами 1) и 2):

$$\begin{aligned} 3^0 &\equiv 1 \pmod 7 \\ 3^1 &\equiv 3 \pmod 7 \\ 3^2 &\equiv 2 \pmod 7 \\ 3^3 &\equiv 6 \pmod 7 \\ 3^4 &\equiv 4 \pmod 7 \\ 3^5 &\equiv 5 \pmod 7. \end{aligned}$$

Составляем таблицу для нахождения индексов по числам:

n	1	2	3	4	5	6
$\operatorname{ind}_3 n$	0	2	1	4	5	3

На основе полученной таблицы можно составить таблицу для нахождения числа по его индексу:

$\operatorname{ind}_3 n$	0	1	2	3	4	5
n	1	3	2	6	4	5

3. Применение индексов к решению сравнений.

а) Решение сравнений первой степени по простому модулю.

Пусть дано сравнение первой степени по простому модулю

$$ax \equiv b \pmod p,$$

где $(a,\ p) = 1$. «Индексируем» левую и правую части этого сравнения. Получим:

$$\operatorname{ind} a + \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1}.$$

(основание индексов k при этом нас не интересует, поскольку переходить к другому основанию нет необходимости).

Далее имеем:

$$\operatorname{ind} x \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}.$$

Находя по таблицам $\operatorname{ind} a = \gamma_1$ и $\operatorname{ind} b = \gamma_2$ (по модулю p) и заменяя при необходимости число $\gamma_2 - \gamma_1$ наименьшим неотрицательным вычетов γ из класса $\overline{\gamma_2 - \gamma_1}$ вычетов по модулю $p-1$, получим сравнение

$$\operatorname{ind} x \equiv \gamma \pmod{p-1},$$

равносильное исходному. Число γ является индексом по модулю p некоторого числа c, находя которое по таблице «антиндексов», перепишем последнее сравнение в виде

$$\operatorname{ind} x \equiv \operatorname{ind} c \pmod{p-1}.$$

«Потенцируя» его, получим решение исходного сравнения

$$x \equiv c \pmod{p}.$$

З а д а ч а 5. Решить сравнение $4x \equiv -2 \pmod 7$.

Р е ш е н и е. Вычет -2 заменяем положительным вычетом по модулю 7 и получаем сравнение: $4x \equiv 5 \pmod 7$. Имеем $(4,\ 7) = 1$, следовательно сравнение имеет единственный класс решений. Индексируя левую и правую часть сравнения, будем иметь:

$$\operatorname{ind} 4 + \operatorname{ind} x \equiv \operatorname{ind} 5 \pmod 6.$$

По таблице индексов (см. пример пункта 2) находим, что $\operatorname{ind}_3 5 = 5$ и $\operatorname{ind}_3 4 = 4$. Тогда

$$\operatorname{ind}_3 x \equiv 1 \pmod 6.$$

Теперь, наконец, по таблицам «антиндексов» находим, что $x \equiv 3 \pmod 7$.

б) Решение двучленных сравнений по простому модулю.

О п р е д е л е н и е 2. Сравнение вида

$$ax^n \equiv b \pmod{p}, \tag{67}$$

где $a \not\equiv 0 \pmod{p}$ и $n \in \mathbb{N}$, называется *двучленным сравнением n-ой степени по простому модулю с одним неизвестным.*

Индексируя обе части сравнения (67), получим равносильное сравнение:

$$\operatorname{ind} a + n \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1}.$$

Обозначая $\operatorname{ind} x = z$, $\operatorname{ind} b - \operatorname{ind} a = c$, приходим к сравнению

$$nz \equiv c \pmod{p-1}. \tag{68}$$

Таким образом, решение сравнения (67) сводится к решению сравнения (68) первой степени. Если $(n,\ p-1) = d$ и $c \vdots d$, то сравнение (68), а, следовательно, и сравнение (67), имеет d решений; если же $c \not\vdots d$, то сравнение (68), а потому и сравнение (67), решений не имеет.

З а д а ч а 6. Решить сравнение $2x^5 \equiv 3 \pmod{7}$

Р е ш е н и е. «Индексируем» обе части сравнения:

$$\operatorname{ind} 2 + 5\operatorname{ind} x \equiv \operatorname{ind} 3 \pmod{6} \Leftrightarrow$$

$$\Leftrightarrow 5\operatorname{ind} x \equiv \operatorname{ind} 3 - \operatorname{ind} 2 \pmod{6} \Leftrightarrow$$

$$\Leftrightarrow 5\operatorname{ind} x \equiv 1 - 2 \pmod{6} \Leftrightarrow$$

$$\Leftrightarrow 5\operatorname{ind} x \equiv -1 \pmod{6} \Leftrightarrow$$

$$\Leftrightarrow 5\operatorname{ind} x \equiv 5 \pmod{6}, \quad (5,\ 6) = 1 \Leftrightarrow$$

$$\Leftrightarrow \operatorname{ind} x \equiv 1 \pmod{6} \Leftrightarrow$$

$$\Leftrightarrow x \equiv 3 \pmod{7}.$$

в) Решение двучленных показательных сравнений по простому модулю.

Ограничимся рассмотрением показательного сравнения вида:

$$a \cdot c^x \equiv b \pmod{p}, \tag{69}$$

где $(a,\ p) = 1$ и $(c,\ p) = 1$.

«Индексируя» обе части сравнения (69), получим равносильное ему сравнение:

$$\operatorname{ind} a + x \operatorname{ind} c \equiv \operatorname{ind} b \pmod{p-1},$$

или

$$x \operatorname{ind} c \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}. \tag{70}$$

Сравнение (70) является сравнением первой степени по модулю $p-1$. Если $(\operatorname{ind} c,\ p-1) = d$ и $(\operatorname{ind} b - \operatorname{ind} a) \vdots d$, то сравнение (70), а следовательно и сравнение (69) имеет d решений; если же $(\operatorname{ind} b - \operatorname{ind} a) \not\vdots d$, то сравнение (70), а следовательно и сравнение (69), решений не имеет.

З а м е ч а н и е. Если $a \vdots p$ или $c \vdots p$, а $b \not\vdots p$, то сравнение (69) невозможно и, следовательно, решений иметь не будет; если же при этом и $b \vdots p$, то сравнение (69) будет сводиться к тождественному сравнению вида $0^x \equiv 0 \pmod{p}$, которое будет удовлетворяться любым значением x.

З а д а ч а 7. Решить сравнение $5^x \equiv 3 \pmod{7}$.

Р е ш е н и е. Имеем: $x \operatorname{ind} 5 \equiv \operatorname{ind} 3 \pmod{6}$, или

$$5x \equiv 1 \pmod{6} \Leftrightarrow$$

$$\Leftrightarrow 5x \equiv 25 \pmod{6}, \quad (5,\ 6) = 1 \Leftrightarrow$$

$$\Leftrightarrow x \equiv 5 \pmod{6}.$$

Это решение и будет единственным решением данного сравнения.

7. ПРАКТИКУМ ПО ТЕОРИИ ЧИСЕЛ

Практическое занятие №1
Числовые функции $\{x\}$, $[x]$, $\tau(x)$, $\sigma(x)$, $\mu(x)$. Распределение простых чисел

1. Найти показатель, с которым число $p = 3$ входит в произведения 100!, 250!.
2. Сколькими нулями оканчивается число 100! ?
3. Разложить на простые множители 10!, 25!.
4. Вычислить $\tau(n)$ и $\sigma(n)$ для чисел:
   а) $n = 375$;
   б) $n = 720$;
   в) $n = 957$;
   г) $n = 988$;
   д) $n = 1200$.
5. Найти все делители чисел:
   а) $n = 360$;
   б) $n = 186$.
6. Число n имеет только два простых делителя, причем $\tau(n) = 6,\ \sigma(n) = 28$. Найти n.
7. Исследовать, какие из чисел, заключенных между 2320 и 2350, являются простыми.
8. Докажите мультипликативность числовых функций $\tau(n)$ и $\sigma(n)$. Указание: воспользуйтесь определением мультипликативной функции и основной теоремой арифметики.
9. Вычислить: $\mu(60)$, $\mu(323)$, $\mu(231)$.
10. Справедлива ли теорема Дирихле для арифметических прогрессий:
    а) $4,\ 12,\ 20,\ 28,\ \ldots$;

б) 5, 9, 13, 17, ...?

Почему?

11. Можно ли утверждать, ссылаясь на теорему Дирихле, что множество простых чисел вида:

а) $5t + 1, t \in \mathbb{N}$;

б) $6t + 3, t \in \mathbb{N}$; бесконечно? Почему?

Практическое занятие №2
Систематические числа и действия над ними

1. Запишите все цифры шестнадцатеричной системы счисления.

2. Верно ли записаны числа в семеричной системе счисления: 1254_7, 3712_7, 38421_7, 17289_7?

3. Запишите число 12 в системах счисления с основаниями 2, 3, 4, 5, 6, 7, 8.

4. Чему равно основание системы счисления, в которой $26 = 101_x$?

5. Имеют ли место следующие равенства: $345_6 = 1243_4$, $147_8 = 23621_3$?

6. Найдите цифры для записи чисел в указанных системах счисления:

а) $37051_8 = x_5$;

б) $42013_4 = x_7$;

в) $7981_{10} = x_9$;

г) $42121_7 = x_{12}$.

7. Выполните указанные действия:

а) $3487_9 + 8765_9$;

б) $40(10)8_{12} + 31(11)9_{12}$;

в) $132_5 \cdot 14_5$;

г) $(11)26_{12} \cdot 32_{12}$;

д) $4704_8 \div 31_8$.

Практическое занятие №3
Контрольная работа по темам «Числовые функции» и «Систематические числа»

1. Вычислить $\tau(n)$, $\sigma(n)$ и $\mu(n)$, если

   1) $n = 1120$; 2) $n = 968$;

   3) $n = 896$; 4) $n = 1256$;

   5) $n = 728$; 6) $n = 987$;

   7) $n = 1126$; 8) $n = 936$;

   9) $n = 1058$; 10) $n = 1210$.

2. Выполнить указанные действия:

   1) $2314_5 \div 45_7$; 2) $1322_6 \div 31_8$;

   3) $2114_7 \div 21_5$; 4) $2431_5 \div 42_6$;

   5) $1502_6 \div 13_5$; 6) $3124_5 \div 21_7$;

   7) $2415_7 \div 42_6$; 8) $1561_8 \div 52_6$;

   9) $4102_6 \div 17_8$; 10) $3251_8 \div 32_5$.

Дополнительные задания
(общие для всех вариантов)

3. Найти количество натуральных чисел от 120 до 315, делящихся на 11.

4. Выполнить указанные действия:

   а) $(361_7 + 24_5) \cdot 131_6$;

   б) $(1241_6 - 38_9) \div 12_3$;

   в) $2146_8 \div 32_5 - 134_6$.

Практическое занятие №4
Цепные дроби и рациональные числа. Подходящие дроби и их свойства

1. Разложите рациональные числа в цепные дроби:

а) $\frac{343}{226}$; б) $\frac{226}{343}$; в) $\frac{117}{343}$; г) $-\frac{343}{117}$.

Сравните подходящие дроби в этих разложениях.

2. Преобразуйте в обыкновенную дробь следующие цепные дроби:

а) $[2;\ 3,\ 1,\ 4]$;

б) $[2;\ 1,\ 1,\ 2,\ 1,\ 6,\ 2,\ 5]$;

в) $[0;\ 1,\ 2,\ 3,\ 4,\ 5]$;

г) $[-2;\ 3,\ 1,\ 3,\ 4,\ 2]$.

3. Сократите дроби с помощью разложения в цепную дробь:

а) $\frac{1043}{3427}$; б) $\frac{3587}{2743}$; в) $\frac{1857}{9153}$; г) $\frac{70757}{491209}$.

4. С помощью подходящих дробей найдите приближение к дроби $\frac{a}{b} = \frac{13891}{5065}$ с точностью до: а) 0,001; б) 0,0001.

5. Разложите 0,429 в непрерывную дробь и найдите третье приближение.

Практическое занятие №5
Квадратичные иррациональности и бесконечные цепные дроби

1. Квадратичные иррациональности представьте бесконечными периодическими цепными дробями:

а) $\alpha = \sqrt{12}$; б) $\alpha = \dfrac{1+\sqrt{3}}{2}$; в) $\alpha = 1+\sqrt{7}$;

г) $\alpha = \sqrt{3}$; д) $\alpha = \sqrt{6}$; е) $\alpha = \dfrac{2+\sqrt{5}}{3}$.

2. Найти квадратичные иррациональности по их разложениям в периодические цепные дроби:

а) $[(1;\ 2,\ 4,\ 6)]$; б) $[2;\ (1,\ 1,\ 1,\ 4)]$;

в) $[(2;\ 2,\ 1,\ 1)]$.

3. При помощи цепных дробей вычислить с точностью до 0,0001 оба корня каждого из следующих квадратных уравнений:

а) $x^2 - 9x + 6 = 0$;

б) $2x^2 - 3x - 6 = 0$.

4. Найти для разложения $e = 2{,}718281828\ldots$ в цепную дробь ее неполные частные до q_6 и подходящие дроби до $\dfrac{P_6}{Q_6}$; оценить погрешность для $\dfrac{P_6}{Q_6}$ и выразить эту подходящую дробь в виде десятичной дроби.

5. Среди подходящих дробей разложения α найти наилучшее приближение α со знаменателем $Q \leqslant b$ и оценить допущенную погрешность ε:

а) $\alpha = \dfrac{\sqrt{77}-3}{2},\ Q \leqslant 100$;

б) $\alpha = \dfrac{\sqrt{35}+1}{2},\ Q \leqslant 100$;

в) $\alpha = \dfrac{22+\sqrt{15}}{7},\ Q \leqslant 100$;

г) $\alpha = \dfrac{\sqrt{21}+1}{2},\ Q \leqslant 50$.

Практическое занятие №6
Контрольная работа по теме «Цепные дроби»

1. Преобразовать в обыкновенные дроби следующие непрерывные дроби:

1) $[2;\ 3,\ 2,\ 4,\ 2]$;
2) $[3;\ 1,\ 2,\ 6,\ 2]$;
3) $[4;\ 2,\ 3,\ 1,\ 2]$;
4) $[3;\ 3,\ 1,\ 2,\ 3]$;
5) $[2;\ 5,\ 1,\ 2,\ 2]$;
6) $[2;\ 4,\ 1,\ 2,\ 1]$;
7) $[3;\ 2,\ 2,\ 2,\ 3]$;
8) $[2;\ 2,\ 2,\ 1,\ 2]$;
9) $[4;\ 3,\ 3,\ 1,\ 3]$;
10) $[4;\ 1,\ 2,\ 6,\ 2]$.

2. С помощью подходящих дробей найти приближение к данной дроби с точностью до 0,001.

1) $\dfrac{12126}{5386}$;
2) $\dfrac{13891}{5065}$;
3) $\dfrac{3587}{2743}$;
4) $\dfrac{9153}{1857}$;
5) $\dfrac{2741}{3287}$;
6) $\dfrac{12621}{4283}$;
7) $\dfrac{10213}{5327}$;
8) $\dfrac{3489}{2747}$;
9) $\dfrac{3027}{4325}$;
10) $\dfrac{5621}{3787}$.

Дополнительные задания (общие для всех вариантов)

3. Сократить дробь $\dfrac{3653}{3107}$, используя разложение ее в цепную дробь.

4. Не разлагая действительное число α в цепную дробь, установить, может ли оно иметь подходящую дробь δ?

Значения α и δ: 1) $\alpha = \sqrt{10}$, $\delta = \dfrac{16}{6}$; 2) $\alpha = \sqrt{7}$, $\delta = \dfrac{37}{14}$.

Практическое занятие №7
Числовые сравнения. Кольцо классов вычетов по составному модулю и поле по простому модулю

1. Среди чисел 217, 42, 182, 241 найти все пары чисел, сравнимых между собой по модулю 12.
2. Можно ли рассматривать систему целых чисел

$$2,\ 9,\ 16,\ 20,\ 27,\ 39,\ 46,\ 85$$

как полную систему вычетов по модулю 8?
3. Написать полные системы абсолютно наименьших вычетов по модулям 10 и 16.
4. Записать приведенные системы вычетов по модулям 11 и 45.
5. Найти все обратимые элементы кольца $\langle \mathbb{Z}_{12},\ \oplus,\ \odot \rangle$.
6. Какие из колец $\langle \mathbb{Z}_5,\ \oplus,\ \odot \rangle$, $\langle \mathbb{Z}_8,\ \oplus,\ \odot \rangle$, $\langle \mathbb{Z}_{11},\ \oplus,\ \odot \rangle$, $\langle \mathbb{Z}_{20},\ \oplus,\ \odot \rangle$ являются полями?

Практическое занятие №8
Функция Эйлера и ее свойства

1. Вычислить значение функции Эйлера для чисел:
   а) $n = 375$;
   б) $n = 720$;
   в) $n = 4320$;
   г) $n = 998$;
   д) $n = 1200$.
2. Известно, что $\varphi(a) = 3600$. Найти a, если $a = 3^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma}$.
3. Сколько натуральных чисел, не взаимно простых с числом 120, содержится в интервале $[1;\ 120]$?

4. Доказать, что если $n \geqslant 3$, то $\varphi(n)$ — четное число.

5. На основании свойств функции Эйлера доказать, что в натуральном ряду существует бесконечное множество простых чисел.

6. Найти условия, при которых $\varphi(3x) = \varphi(2x)$, $x \in \mathbb{N}$.

Практическое занятие №9
Функция Эйлера. Теорема Эйлера и Ферма

1. Найти последние цифры в записи чисел:
   а) 123^{45}; б)11^{203}; в)7^{1199}; г)49^{341}.
2. Найти остаток от деления:
   а) числа 125^{49} на число 7;
   б) числа 349^{126} на число 11;
   в) числа 12123^{54} на число 13;
   г) числа 3^{157} на число 100;
   д) числа 11^{1201} на число 1000.
3. Найти две последние цифры в записи чисел:
   а) 17^{61}; б)19^{79}; в)23^{114}; г)97^{203}.
4. Показать, что:
   а) $1^{16} + 3^{16} + 7^{16} + 9^{16} \equiv 4 \pmod{10}$;
   б) $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv -1 \pmod{7}$.

Практическое занятие №10
Контрольная работа по теме «Числовые сравнения»

1. Записать приведенную систему вычетов по модулю 27.

2. Найти все обратимые элементы кольца $\langle \mathbb{Z}_{16}, \oplus, \odot \rangle$.

3. Найти остаток от деления числа 345^{126} на 7.

4. Найти последнюю цифру в записи числа 98^{32}.

5. Вывести признак делимости на 7.

Практическое занятие №11
Сравнения с неизвестной величиной. Сравнения первой степени

1. Решить сравнения:

а) $2x \equiv 3 \pmod 5$; б) $3x \equiv 4 \pmod 7$;

в) $7x \equiv 10 \pmod{11}$; г) $12x \equiv 7 \pmod{13}$;

д) $7x \equiv 11 \pmod{15}$; е) $10x \equiv 15 \pmod{25}$;

ж) $9x \equiv 12 \pmod{21}$; з) $14x \equiv 4 \pmod 8$;

и) $4x \equiv 18 \pmod{24}$; к) $28x \equiv 40 \pmod{44}$.

2. Составьте сравнение первой степени по модулю 21: а) имеющее одно решение; б) имеющее 3 или 7 решений; в) имеющее 2, 10, 15 решений.

Практическое занятие №12
Диофантовы уравнения, методы их решения

1. Решить диофантовы уравнения:

а) $13x + 16y = 19$; б) $21x + 30y = 39$;

в) $15x + 45y = 120$; г) $14x + 21y = 100$;

д) $129x + 48y = 342$; е) $12x + 16y = 428$.

2. Решить диофантовы уравнения с помощью цепных дробей:

а) $11x + 19y = 113$; б) $13x + 29y = 124$.

3. Сумма произведений двух целых чисел соответственно на 7 и на 3 равна 41. Найти эти числа.

4. Для настилки пола шириной в 3 метра имеются доски шириной в 11 см и 13 см. Сколько нужно взять досок того и другого размера?

Практическое занятие №13
Системы сравнений, методы их решения

1. Решить системы сравнений первой степени:

а) $\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 5 \pmod{7} \end{cases}$; б) $\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 7 \pmod{25} \end{cases}$;

в) $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 3 \pmod{10} \\ x \equiv 5 \pmod{3} \end{cases}$; г) $\begin{cases} x \equiv 13 \pmod{16} \\ x \equiv 3 \pmod{10} \\ x \equiv 9 \pmod{14} \end{cases}$;

д) $\begin{cases} 7x \equiv 4 \pmod{15} \\ 3x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{9} \end{cases}$; е) $\begin{cases} 17x \equiv 7 \pmod{2} \\ 2x \equiv 1 \pmod{3} \\ 2x \equiv 2 \pmod{5} \end{cases}$.

2. Найти числа, которые при делении на

а) 4, 5, 7 дают соответственно остатки 2, 3, 4;

б) 13, 21, 23 дают соответственно остатки 9, 1, 13;

в) 2, 3, 4, 5 дают соответственно остатки 1, 1, 1, 0.

3. Между 500 и 800 найдите все натуральные числа, которые при делении на 3, 5, 8 дают соответственно остатки 2, 3, 4.

Практическое занятие №14
Сравнения высших степеней. Квадратичные вычеты и невычеты

1. Заменить данные сравнения равносильными им сравнениями и решить их:

а) $x^{10} + 3x^5 - 4x^3 + x^2 - 3 \equiv 0 \pmod 7$;

б) $x^{14} - x^{12} + 3x^5 - 6x^2 + x + 1 \equiv 0 \pmod{11}$;

в) $x^8 - 3x^7 + 2x^6 + 3x^4 - 2x^2 - 1 \equiv 0 \pmod 5$;

г) $x^{13} - x^3 + x - 3 \equiv 0 \pmod{11}$;

д) $x^9 - 3x^4 + 2x^3 - x + 3 \equiv 0 \pmod 7$.

2. Решить сравнения:

а) $x^{14} - 4x^{13} - x + 6 \equiv 0 \pmod{13}$;

б) $x^{12} + 2x^{11} - 2x - 1 \equiv 0 \pmod{11}$;

в) $x^9 - x^3 + x - 5 \equiv 0 \pmod 7$.

3. Разложить многочлены на множители по модулю p:

а) $f(x) = x^3 - 8x^2 - x + 3, \quad p = 11$;

б) $f(x) = x^4 - 4x^3 + 4x - 1, \quad p = 7$;

в) $f(x) = x^4 + 6x^3 - 3x^2 + x + 2, \quad p = 13$.

4. Найти все квадратичные вычеты и невычеты по модулю 19.

5. С помощью критерия Эйлера установить, какие из чисел 3, 5, 7, 8 являются квадратичными вычетами по модулю 13.

6. С помощью критерия Эйлера установить, имеют ли решения сравнения:

а) $x^2 \equiv 7 \pmod{11}$;

б) $x^2 \equiv 12 \pmod{13}$;

в) $x^2 \equiv 5 \pmod 7$;

г) $x^2 \equiv 6 \pmod{13}$;

д) $x^2 \equiv 5 \pmod{11}$;

е) $x^2 \equiv 3 \pmod{29}$;

ж) $x^2 \equiv 7 \pmod{17}$;

з) $x^2 \equiv 3 \pmod 7$.

7. Доказать, что ни при каком целом значении x выражение $x^2 + 3x + 5$ не делится на 121.

Практическое занятие №15
Показатели и их свойства

1. Какому показателю принадлежат:
   а) число 7 по модулю 12;
   б) число 3 по модулю 17;
   в) число 6 по модулю 10;
   г) число 25 по модулю 31;
   д) число 5 по модулю 61.
2. Распределить все классы чисел по показателям:
   а) по модулю 7;
   б) по модулю 11;
   в) по модулю 13.
3. Найти все классы вычетов, принадлежащие показателям:
   а) $\delta = 5$ по модулю 11;
   б) $\delta = 6$ по модулю 13;
   в) $\delta = 9$ по модулю 19.

Практическое занятие №16
Первообразные корни по простому модулю, алгоритм нахождения первообразных корней. Индексы. Решение сравнений с помощью индексов

1. Найти все первообразные корни:
   а) по модулю 5;
   б) по модулю 7;
   в) по модулю 53.
2. Составить таблицу индексов:
   а) по модулю 11;

б) по модулю 19.

3. Решить сравнения с помощью индексов:

а) $17x \equiv 20 \pmod{19}$; б) $23x \equiv 17 \pmod{11}$;
в) $15x^4 \equiv 26 \pmod{29}$; г) $13x^{21} \equiv 5 \pmod{31}$;
д) $x^2 \equiv 89 \pmod{97}$; е) $40x^{10} \equiv 3 \pmod{17}$;
ж) $12^x \equiv 7 \pmod{19}$; з) $6^x \equiv -3 \pmod{11}$;
и) $2^x \equiv 7 \pmod{67}$; к) $15 \cdot 7^{2x} \equiv 8 \cdot 3^{3x} \pmod{31}$.

4. С помощью таблиц индексов найти остатки от деления:

а) числа 13^{19} на 19; б) числа 3^{18} на 11;
в) числа 19^{32} на 17; г) числа 29^{117} на 23.

Практическое занятие №17
Контрольная работа по темам «Сравнения с неизвестной величиной» и «Степенные вычеты»

1. Решить сравнения первой степени:

1) $126x \equiv 41 \pmod{21}$; 2) $221x \equiv 11 \pmod{23}$;
3) $129x \equiv 25 \pmod{15}$; 4) $136x \equiv 27 \pmod{15}$;
5) $248x \equiv 27 \pmod{13}$; 6) $158x \equiv 42 \pmod{17}$;
7) $242x \equiv 72 \pmod{11}$; 8) $315x \equiv 49 \pmod{15}$;
9) $256x \equiv 17 \pmod{13}$; 10) $405x \equiv 11 \pmod{17}$.

2. Решить уравнения в целых числах:

1) $81x - 48y = 33$; 2) $17x - 19y = 120$;
3) $23x + 10y = 310$; 4) $11x + 23y = 117$;
5) $10x - 12y = 86$; 6) $14x - 8y = 78$;
7) $22x + 13y = 128$; 8) $40x + 12y = 321$;
9) $16x - 22y = 141$; 10) $18x + 23y = 160$.

3. Решить системы сравнений первой степени:

$$1)\ \begin{cases} 2x \equiv 7 \pmod 5 \\ x \equiv -3 \pmod 4 \\ x \equiv 13 \pmod 7 \end{cases};$$

$$2)\ \begin{cases} 3x \equiv -5 \pmod 7 \\ x \equiv 13 \pmod 4 \\ x \equiv -6 \pmod{11} \end{cases};$$

$$3)\ \begin{cases} x \equiv 14 \pmod{19} \\ x \equiv 5 \pmod 7 \\ x \equiv -9 \pmod{10} \end{cases};$$

$$4)\ \begin{cases} x \equiv 5 \pmod{13} \\ 2x \equiv 7 \pmod{10} \\ x \equiv -2 \pmod 7 \end{cases};$$

$$5)\ \begin{cases} 4x \equiv -1 \pmod{11} \\ x \equiv 7 \pmod 5 \\ x \equiv -10 \pmod 7 \end{cases};$$

$$6)\ \begin{cases} -x \equiv 4 \pmod 5 \\ x \equiv 10 \pmod 7 \\ x \equiv -3 \pmod{11} \end{cases};$$

$$7)\ \begin{cases} 2x \equiv 11 \pmod 3 \\ x \equiv -2 \pmod{13} \\ x \equiv 10 \pmod 4 \end{cases};$$

$$8)\ \begin{cases} x \equiv 12 \pmod 7 \\ x \equiv -4 \pmod 5 \\ x \equiv 3 \pmod{13} \end{cases};$$

$$9)\ \begin{cases} 2x \equiv 1 \pmod 5 \\ x \equiv -5 \pmod 7 \\ x \equiv 17 \pmod 6 \end{cases};$$

$$10)\ \begin{cases} x \equiv 13 \pmod{11} \\ x \equiv -10 \pmod 7 \\ x \equiv 14 \pmod{13} \end{cases}.$$

4. Найти все первообразные корни:

1) по модулю 11; 2) по модулю 13;
3) по модулю 17; 4) по модулю 19;
5) по модулю 23; 6) по модулю 29;
7) по модулю 41; 8) по модулю 43;
9) по модулю 47; 10) по модулю 31.

5. Составить таблицу индексов по модулю 17 и решить сравнения:

1) $12x^5 \equiv 6 \pmod{17}$; 2) $10x^4 \equiv 7 \pmod{17}$;
3) $3^x \equiv 10 \pmod{17}$; 4) $5^x \equiv 12 \pmod{17}$;
5) $13x^6 \equiv 2 \pmod{17}$; 6) $6^x \equiv 13 \pmod{17}$;
7) $3x^7 \equiv 12 \pmod{17}$; 8) $6x^3 \equiv 13 \pmod{17}$;
9) $7^x \equiv 5 \pmod{17}$; 10) $10^x \equiv 3 \pmod{17}$.

8. ГЛОССАРИЙ

Алгебраическое число — комплексное или действительное число, являющееся корнем некоторого многочлена с целыми коэффициентами, одновременно отличными от нуля.

Индекс класса вычетов $\overline{x}$ по модулю p при основании $\overline{k}$ — число γ, такое, что $\overline{k^\gamma} = \overline{x}$, где p — простое число и $\overline{k}$ — первообразный корень по модулю p.

Линейное диофантово уравнение с двумя переменными — уравнение вида

$$ax + by = c, \quad (a,\ b,\ c \in \mathbb{Z}, a,\ b \neq 0),$$

под частным решением которого понимается пара целых чисел $x_0,\ y_0$, таких, что при подстановке их в уравнение соответственно вместо x и y получается верное равенство.

Мультипликативная функция — числовая функция, удовлетворяющая требованиям:

1. Функция определена $\forall n \in \mathbb{N}$, причем $f(1) = 1$;
2. $\forall n,\ m \in \mathbb{N},\ (n,\ m) = 1 \quad f(n \cdot m) = f(n) \cdot f(m)$.

Неравенство Чебышева — неравенство, выражающее асимптотический закон распределения простых чисел:

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

Отношение сравнимости по модулю — отношение равноостаточных целых чисел при делении на одно и то же натуральное число ($a \equiv b \pmod{m}$).

Первообразный корень по простому модулю — класс вычетов $\overline{a}$ по модулю p, принадлежащий показателю $\delta = p - 1$.

Подходящая дробь — любой «отрезок» цепной дроби.

Полная система классов вычетов по модулю m — совокупность всех классов вычетов по модулю m.

Порядок класса вычетов $\overline{k}$, взаимно простого с модулем m, — наименьшее натуральное число δ, такое, что $\overline{k^\delta} = \overline{1}$.

Приведенная система классов вычетов по модулю m — совокупность всех классов вычетов по модулю m, взаимно простых с m.

Решето Эратосфена — способ нахождения положительных простых чисел, не превосходящих заданное натуральное число.

Сравнение второй степени по простому модулю — сравнение вида $x^2 \equiv a \pmod{p}$.

Сравнение первой степени с одной переменной — сравнение вида: $ax \equiv b \pmod{m}$.

Трансцендентное число — любое неалгебраическое число.

Функция Эйлера — числовая функция, выражающая количество натуральных чисел, не превосходящих заданного числа n и взаимно простых с ним.

9. ЛИТЕРАТУРА

9.1 Основная литература

1. Александров В.А., Горшенин С.М. Задачник-практикум по теории чисел. М.: Просвещение, 2006.
2. Бухштаб А.А. Теория чисел. С.-Пб.: Лань, 2008.
3. Виноградов И.М. Основы теории чисел. М.: Физматлит, 2003.
4. Грибанов П.И., Титов В.У. Сборник упражнений по теории чисел. М.: Просвещение, 2007.
5. Куликов Л.Я. Алгебра и теория чисел. М.: Флинта-Наука, 2001.
6. Михелович Ш.Х. Теория чисел. С.-Пб.: Лань, 2004.

9.2 Дополнительная литература

1. Арнольд И.В. Теория чисел. М.: Учпедгиз, 1939.
2. Архангельская В.М. Элементарная теория чисел: Учебное пособие. Изд. Саратовского университета, 1963.

3. Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. Введение в теорию чисел. М.: Изд-во МГУ, 1995.

4. Кочева Н.А. Задачник-практикум по алгебре и теории чисел. М.: Изд. МГЗПИ, 1984.

5. Ляпин Е.С., Евсеев А.Е. Алгебра и теория чисел. Ч.I. Числа. М.: Просвещение, 1978.

6. Марчевский М.Н. Теория чисел. Харьков, 1958.

7. Нивен А. Числа рациональные и иррациональные. М.: Мир, 1966.

8. Оре О. Приглашение в теорию чисел. М.: Наука, 1980.

9. Серпинский В. 250 задач по элементарной теории чисел. М.: Просвещение, 1968.

10. Сушкевич Я.Н. Теория чисел. Харьков, 1954.

11. Хинчин А.Я. Три жемчужины теории чисел. М.: Наука, 1979.

Для заметок

Для заметок

Учебное издание

Теория чисел

Учебно-методический комплекс

Составители:
Пуркина Валентина Федоровна
Кайгородов Евгений Владимирович

Подписано в печать 11.01.2010. Формат 60 × 84/16
Бумага офсетная. Усл.печ.л. — 13,0
Заказ № 1 . Тираж 50 экз.
РИО Горно-Алтайского госуниверситета,
649000, г. Горно-Алтайск, ул. Ленкина, д. 1
Отпечатано полиграфическим отделом
Горно-Алтайского госуниверситета,
649000, г. Горно-Алтайск, ул. Ленкина, д. 1