ГЛАВНОЕ УПРАВЛЕНИЕ ВЫСШИХ И СРЕДНИХ
ПЕДАГОГИЧЕСКИХ УЧЕБНЫХ ЗАВЕДЕНИЙ
МИНИСТЕРСТВА ПРОСВЕЩЕНИЯ РСФСР

МОСКОВСКИЙ
ГОСУДАРСТВЕННЫЙ
ЗАОЧНЫЙ
ПЕДАГОГИЧЕСКИЙ
ИНСТИТУТ

В. А. АЛЕКСАНДРОВ
С. М. ГОРШЕНИН

ЗАДАЧНИК-ПРАКТИКУМ ПО ТЕОРИИ ЧИСЕЛ

ПРОСВЕЩЕНИЕ

1972

ГЛАВНОЕ УПРАВЛЕНИЕ ВЫСШИХ И СРЕДНИХ ПЕДАГОГИЧЕСКИХ
УЧЕБНЫХ ЗАВЕДЕНИЙ МИНИСТЕРСТВА ПРОСВЕЩЕНИЯ РСФСР

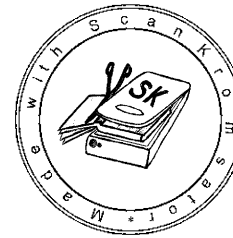
Московский государственный заочный педагогический институт

В. А. АЛЕКСАНДРОВ и С. М. ГОРШЕНИН

ЗАДАЧНИК-ПРАКТИКУМ ПО ТЕОРИИ ЧИСЕЛ

*Для студентов заочных отделений
физико-математических факультетов
педагогических институтов*

ИЗДАНИЕ ТРЕТЬЕ, ПЕРЕРАБОТАННОЕ



ИЗДАТЕЛЬСТВО «ПРОСВЕЩЕНИЕ»
Москва — 1972

Одобрено кафедрой математики Московского государственного заочного педагогического института

Редактор *О. А. Павлович*

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ К ТРЕТЬЕМУ ИЗДАНИЮ

При подготовке третьего издания учитывались требования курса «Алгебра и теория чисел».

По сравнению со вторым изданием осуществлены следующие дополнения: введены упражнения на темы «Решение неопределенных уравнений первой степени с двумя неизвестными в целых числах» и «Конечные цепные дроби»; даны различные методы обоснования признаков делимости чисел; увеличено количество упражнений для самостоятельного решения.

В отличие от предыдущих изданий задачник разбит на две части. В первой части дан минимум упражнений, необходимый для подготовки студентов к выполнению контрольной работы и к зачету (этим упражнениям предшествуют примеры с подробными решениями). Вторая часть включает более сложные задачи, которые, возможно, заинтересуют студентов в процессе изучения курса.

Все дополнения и изменения, о которых шла речь выше, осуществлены вторым из авторов.

С. Горшенин.

ВВЕДЕНИЕ

Настоящий задачник-практикум является учебным пособием для студентов-заочников математических специальностей педагогических институтов. В пособии студент найдет образцы решения задач и материал для упражнений по всем основным разделам курса «Алгебра и теория чисел».

Приступая к работе с задачником-практикумом, студент предварительно должен изучить необходимый теоретический материал. В процессе работы надо обратить особое внимание на выбор наиболее рациональных методов решения упражнений. Сказанное прежде всего относится к решению сравнений и систем сравнений первой степени с одним неизвестным, к нахождению классов чисел, принадлежащих показателю, первообразных корней по простому модулю и др.

Хотя при выборе рациональных методов решения целого ряда задач студент убедится, что применение таблиц индексов значительно упрощает путь решения, ему необходимо овладеть всеми предлагаемыми в задачнике методами, особенно если учесть, что предварительное составление таблиц индексов — весьма трудоемкий процесс.

Одним из арифметических приложений теории сравнений является нахождение остатка от деления данного числа k на число l; при выполнении упражнений такого характера в задачнике-практикуме в основном используется сравнение:

$$k \equiv z \pmod{l},$$

где z — наименьший неотрицательный вычет по модулю l, который и является искомым остатком.

В разделе «Арифметические приложения теории сравнений» рассматриваются упражнения, отвечающие содержанию этого раздела программы. Студент-заочник должен уяснить, что изучением этого раздела не исчер-

пывается круг арифметических приложений теории чисел (отчасти и теории сравнений). Этим же целям служат приложения различных рассматриваемых в теории чисел числовых функций, теоремы Эйлера о сравнениях, малой теории Ферма, системы сравнений с одним неизвестным и др.

По каждому разделу программы в задачнике указана соответствующая литература. В основу положены следующие курсы:

1. Ш. Х. Михелович. Теория чисел, изд. 2, перераб. и доп. М., «Высшая школа», 1967.

2. А. А. Бухштаб. Теория чисел, изд. 2, испр. М., «Просвещение», 1966.

ЧАСТЬ I

ЗАДАЧИ С РЕШЕНИЯМИ. ЗАДАЧИ ДЛЯ САМОСТОЯТЕЛЬНОГО РЕШЕНИЯ

§ 1. КЛАССЫ ПО ДАННОМУ МОДУЛЮ. СРАВНЕНИЯ И КЛАССЫ

Ш. Х. Михелович. Теория чисел, стр. 36—60.
А. А. Бухштаб. Теория чисел, стр. 72—99.

Вопросы для самопроверки

1. Когда два числа a и b сравнимы по модулю m?
2. Сформулируйте основные свойства сравнений.
3. В чем заключается условие, необходимое и достаточное для того, чтобы два числа a и b принадлежали к одному классу по данному модулю m?
4. Что называется полной системой вычетов по данному модулю m?
5. Что называется приведенной системой вычетов по данному модулю m?
6. Дайте определение функции Эйлера $\varphi(n)$.
7. Сформулируйте основные свойства функции Эйлера.
8. Как читается теорема Эйлера?
9. Как читается малая теорема Ферма?

Разберите решения следующих примеров.

Пример 1. Даны три числа: 78, 210 и 346. Сравнимы ли они с 27 по модулю 11?

Решение. Вычтем из данных чисел 27. Получим числа 51, 183 и 319. Из этих трех чисел только 319 делится на 11, а поэтому только 346 сравнимо с 27 по модулю 11, т. е.

$$346 \equiv 27 \pmod{11}.$$

Пример 2. Показать, что $3^{121} \not\equiv 11 \pmod{21}$.

Решение. Известно, что, если

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

то

$$(a, m) = (b, m).$$

В данном случае имеем:

$$(3^{121}, 21) = 3,$$

но (11, 21) = 1, следовательно,

$$3^{121} \not\equiv 11 \pmod{21}.$$

Пример 3. Дана совокупность чисел

$$(9, 2, 16, 20, 27, 39, 46, 85).$$

Можно ли рассматривать данную совокупность как полную систему вычетов по модулю 8?

Решение. В соответствии с определением полной системы вычетов по модулю m совокупность соответствующих чисел при делении на m должна давать в остатке числа

$$0, 1, 2, 3, 4, \ldots, m-1.$$

Легко установить, осуществляя последовательно деление чисел данной совокупности на число 8, что остатки будут равны числам

$$1, 2, 0, 4, 3, 7, 6, 5,$$

а следовательно, данную совокупность можно рассматривать как полную систему вычетов по модулю 8.

Пример 4. Дана совокупность чисел

$$(9, 2, 16, 20, 27, 39, 46, 86).$$

Осуществить такую замену чисел этой совокупности, чтобы ее можно было принять за полную систему вычетов по модулю 8.

Решение. Сравнивая данную последовательность с последовательностью в примере 3, замечаем, что они отличаются только последним числом, и теперь уже два числа (46 и 86) дают в остатке при делении на 8 число 6. Чтобы получить нужную совокупность, надо заменить одно из них, например число 86, любым другим числом, дающим в остатке при делении на 8 число 5 (например, числом 85).

Пример 5. Написать полные системы абсолютно наименьших вычетов по модулям 7 и 8.

Решение. Если модуль m — нечетное число, то в искомой системе вычетов допустимо наибольшее по абсолютной величине число $\frac{m-1}{2}$; если m — четное число, то $-\frac{m}{2}$. Искомыми полными системами абсолютно наименьших вычетов будут системы: (—3, —2, —1, 0, 1, 2, 3),

если модуль равен 7, и (—3, —2, —1, 0, 1, 2, 3, 4) или (—4, —3, —2, —1, 0, 1, 2, 3), если модуль равен 8.

Пример 6. Дана полная система вычетов (9, 2, 16, 20, 27, 39, 46, 85) по модулю 8. Выбрать из этих чисел те, которые входят в приведенную систему вычетов по модулю 8.

Решение. В соответствии с определением из данной совокупности следует выбрать все числа, которые взаимно просты с модулем. Поэтому приведенная система вычетов по модулю 8 будет иметь еще вид: (9, 27, 39, 85).

Заметим, что приведенная система вычетов по модулю m содержит $\varphi(m)$ чисел; $\varphi(8)=4$, т. е. искомая система должна содержать четыре числа.

Пример 7. Девятая степень однозначного числа n оканчивается цифрой 7; найти это число.

Решение. Так как девятая степень числа n оканчивается цифрой 7, то остаток от деления числа n^9 на 10 должен быть равен 7, что равносильно справедливости сравнения

$$n^9 \equiv 7 \pmod{10}.$$

Так как $(7, 10) = 1$, то $(n, 10) = 1$. Воспользовавшись теоремой Эйлера, получим:

$$n^4 \equiv 1 \pmod{10},$$

где $\varphi(10)=4$.

Возведя обе части последнего сравнения в квадрат, придем к сравнению: $n^8 \equiv 1 \pmod{10}$. Тогда сравнение

$$n^9 \equiv 7 \pmod{10}$$

примет вид:

$$n \equiv 7 \pmod{10},$$

следовательно, $n=7$.

Пример 8. Показать, что

$$1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18} \equiv -1 \pmod{7}.$$

Решение. Воспользуемся малой теоремой Ферма: если $(a, p)=1$, то

$$a^{p-1} \equiv 1 \pmod{p}.$$

Числа 1, 2, 3, 4, 5, 6 взаимно просты с числом 7. На основании указанной теоремы

$$a^6 \equiv 1 \pmod{7}, \qquad (1)$$

где $a=1, 2, 3, 4, 5, 6$.

Сравнение (1) почленно возведем в куб, получим:

$$a^{18} \equiv 1 \pmod 7. \qquad (2)$$

Складывая почленно сравнения вида (2) при $a=1, 2, 3, 4, 5, 6$, имеем:

$$1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18} \equiv 6 \equiv -1 \pmod 7.$$

Замечание. Решение значительно упрощается, если показатель степени есть нечетное число. Пусть требуется показать, что

$$1^{11}+2^{11}+3^{11}+4^{11} \equiv 0 \pmod 5.$$

В левой части сравнения в качестве оснований фигурирует приведенная система наименьших положительных вычетов по модулю 5. В случае нечетных показателей, используя систему абсолютно наименьших вычетов по модулю 5, получим:

$$1^{11}+2^{11}+3^{11}+4^{11} \equiv 1^{11}+2^{11}+(-2)^{11}+ \\ +(-1)^{11} \equiv 0 \pmod 5.$$

Пример 9. Найти остаток от деления числа 7^{402} на 101.

Решение. 101 — простое число. Числа 7 и 101 взаимно просты, а поэтому из малой теоремы Ферма следует, что

$$7^{100} \equiv 1 \pmod{101}.$$

Возведем это сравнение почленно в четвертую степень. Получим:

$$7^{400} \equiv 1 \pmod{101}.$$

Кроме того, $7^2 \equiv 49 \pmod{101}$. Перемножим эти сравнения:

$$7^{402} \equiv 49 \pmod{101}.$$

Из последнего сравнения вытекает, что искомым остатком будет число 49.

Пример 10. Доказать, что кольцо классов по любому простому модулю p не содержит делителей нуля.

Решение. Из высшей алгебры известно, что кольцо содержит делители нуля, если произведение элементов кольца равно нулю кольца, в то время как ни один из сомножителей не равен нулю.

Пусть $\overline{a}$, $\overline{b}$, $\overline{0}$ — классы по простому модулю p; возьмем равенство

$$\overline{a} \cdot \overline{b} = \overline{0},$$

откуда следует справедливость сравнения

$$a \cdot b \equiv 0 \pmod{p}.$$

Так как p — простое число, то либо $a \vdots p$, либо $b \vdots p$, следовательно, соответственно $\overline{a}=\overline{0}$, $\overline{b}=\overline{0}$, и в кольце классов по простому модулю p отсутствуют делители нуля.

Пример 11. Найти последние две цифры числа 243^{402}.

Решение. Очевидно, достаточно найти остаток, полученный при делении числа 243^{402} на 100.

$$243^{402} \equiv 43^{402} \pmod{100}.$$

Но $(43, 100) = 1$, а поэтому

$$43^{\varphi(100)} \equiv 1 \pmod{100},$$

т. е.

$$43^{40} \equiv 1 \pmod{100}.$$

Возведем последнее 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.

Пример 12. Показать, что $(73^{12}-1)$ делится на 105.

Решение. Каноническое разложение числа 105 дает:

$$105 = 3 \cdot 5 \cdot 7.$$

Замечая, что $(73, 3) = (73, 5) = (73, 7) = 1$ и 73 — простое число, применим малую теорему Ферма к числу 73 по модулям 3, 5, 7; получим сравнения:

$$73^2 \equiv 1 \pmod{3},$$
$$73^4 \equiv 1 \pmod{5},$$
$$73^6 \equiv 1 \pmod{7}.$$

Путем возведения обеих частей сравнений в соответствующие степени, получим сравнения:

$$73^{12} \equiv 1 \pmod{3},$$
$$73^{12} \equiv 1 \pmod{5},$$
$$73^{12} \equiv 1 \pmod{7}.$$

Воспользуемся свойством: если некоторое сравнение имеет место по нескольким модулям, то оно справедливо по модулю, являющемуся наименьшим общим кратным данных модулей; следовательно,

$$73^{12} \equiv 1 \pmod{105},$$

откуда

$$(73^{12}-1) \vdots 105.$$

Пример 13. Показать, что число

$$13^{176}-1$$

делится на 89.

Решение. Воспользуемся формулой разложения разности квадратов:

$$13^{176}-1 = (13^{88}-1)(13^{88}+1).$$

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 $(13^{88}-1) \vdots 89$, а следовательно,

$$(13^{176}-1) \vdots 89.$$

Пример 14. Вывести признак делимости числа N на положительное число d, оканчивающееся единицей.

Решение. Запишем число N в виде

$$N = 10a + b,$$

где a — количество десятков, b — цифра единиц числа N; положим $d = 10k+1$.

Пусть справедливо сравнение

$$10a + b \equiv 0 \pmod{10k+1},$$

заметим, что $(k, 10k+1) = 1$. Умножим обе части сравнения на число k, получим:

$$10ak + bk \equiv 0 \pmod{10k+1}.$$

Вычитая из левой части сравнения число $10ak+a$, кратное модулю, приходим к сравнению

$$-a + bk \equiv 0 \pmod{10k+1},$$

откуда

$$a-bk\equiv 0 \pmod{10k+1}.$$

Обратно. Пусть справедливо сравнение

$$a-bk\equiv 0 \pmod{10k+1},$$

откуда

$$-a+bk\equiv 0 \pmod{10k+1}.$$

Прибавим к левой части сравнения число $10ak+a$, кратное модулю, и в результате придем к сравнению

$$10ak+bk\equiv 0 \pmod{10k+1}.$$

Так как $(k, 10k+1)=1$, то, разделив обе части последнего сравнения на число k, получим:

$$10a+b\equiv 0 \pmod{10k+1}.$$

Получен следующий признак делимости: для того чтобы число N делилось на число $d=10k+1$, необходимо и достаточно, чтобы разность между количеством десятков числа N и цифрой единиц числа N, умноженной на число k, делилась на число d.

Заметим, что условие $(k, 10k+1)=1$ используется лишь при доказательстве обратного положения.

Пример 15. Доказать, что если $c \vdots a$, $c \vdots b$, где $(a, b)=1$, то $c \vdots ab$.

Решение. Будем полагать, что a и b — положительные числа; приходим к сравнениям:

$$c\equiv 0 \pmod{a},$$

$$c\equiv 0 \pmod{b}.$$

Учитывая, что $(a, b)=1$, и тот факт, что если одно и то же сравнение имеет место по нескольким модулям, то оно справедливо по модулю, являющемуся наименьшим общим кратным данных модулей, приходим к сравнению

$$c=0 \pmod{ab},$$

откуда

$$c \vdots ab.$$

Пример 16. Установить делимость числа 29463 на число 183.

Решение. Разложим 183 на множители:

$$183=3\cdot 61,$$

при этом $(3, 61)=1$. Легко установить, что число $29463 \vdots 3$.

Применим последовательно признак делимости на число 61. Получим: 2946—18=2928; 292—48=244; но 244 ⋮ 61, следовательно, 29463 ⋮ 183.

Заметим, что процесс может быть продолжен. Если вновь применим признак делимости на 61, в результате получим 24—24=0, 0 ⋮ 61.

Пример 17. Вывести признак делимости числа N на число 19.

Решение. Положим

$$N=10a+b.$$

Пусть справедливо сравнение

$$10a+b=0 \pmod{19};$$

так как $(2, 19)=1$, то, умножая на 2, получим:

$$20a+2b=0 \pmod{19}.$$

Вычитая из левой части число $19a$, кратное модулю, приходим к сравнению

$$a+2b=0 \pmod{19}, \text{ т. е.}$$
$$(a+2b) \vdots 19.$$

Обратно. Пусть справедливо сравнение

$$a+2b=0 \pmod{19}.$$

Прибавляя к левой части число $19a$, кратное модулю, приходим к сравнению

$$20a+2b=0 \pmod{19}.$$

Так как $(2, 19)=1$, то разделим обе части сравнения на число 2. Получим:

$$10a+b \equiv 0 \pmod{19},$$

т. е. $N \vdots 19$.

Получили следующий признак делимости числа N на 19: число N тогда и только тогда делится на число 19, когда сумма количества десятков данного числа и удвоенной цифры единиц данного числа делится на число 19.

Упражнения

1. Среди чисел 216, 134, 214, 303, 21 найти все пары чисел, сравнимых между собой по модулю 5.

2. Среди чисел 135, 106, 181, 225, 167, 452 найти все пары чисел, сравнимых между собой по модулю 15.

3. Среди чисел 217, 42, 182, 241 найти все пары чисел, сравнимых между собой по модулю 12.

4. Даны три числа: 137, 343, 633. Какие из данных чисел сравнимы с числом 13 по модулю 31?

5. Даны три числа: 217, 201, 186. Какие из них сравнимы с числом 11 по модулю 19?

6. Даны три числа: 234, 634, 104. Какие из этих чисел сравнимы с числом 9 по модулю 25?

7. Показать, что сравнения:

а) $11^{207} \equiv 6 \pmod{27}$,

б) $6^{89} \equiv 7 \pmod{16}$,

в) $13^{25} \equiv 5 \pmod{30}$,

г) $7^{101} \equiv 3 \pmod{35}$,

д) $8^{107} \equiv 7 \pmod{14}$

не имеют места.

8. Написать полную систему наименьших положительных вычетов по модулям: а) 6, б) 11, в) 9, г) 13, д) 15.

9. Написать полную систему наименьших неотрицательных вычетов по модулям: а) 5, б) 7, в) 11, г) 12, д) 14.

10. Написать полную систему абсолютно наименьших вычетов по модулям: а) 11, б) 9, в) 7, г) 8, д) 12.

11. Написать приведенную систему вычетов по модулям:

а) 5, б) 7, в) 9, г) 11, д) 12, е) 14, ж) 15.

12. Найти наименьшие положительные вычеты:

а) чисел 113, 127, 41, 47, 53 по модулю 11,

б) чисел 84, 123, 71, 83, 101 по модулю 13,

в) чисел 75, 83, 103, 117, 201 по модулю 15,

г) чисел 63, 88, 97, 105, 136 по модулю 12,

д) чисел 107, 121, 132, 150, 161 по модулю 17.

13. Найти наименьшие неотрицательные вычеты:

а) чисел 115, 131, 57, 48, 83 по модулю 9,

б) чисел 82, 127, 73, 89, 107 по модулю 11,

в) чисел 87, 131, 97, 103, 111 по модулю 12,

г) чисел 69, 93, 100, 123, 141 по модулю 13,

д) чисел 75, 89, 102, 137, 151 по модулю 15.

14. Найти абсолютно наименьшие вычеты:

а) чисел 108, 123, 201, 75, 83 по модулю 10,

б) чисел 97, 138, 61, 87, 151 по модулю 11,

в) чисел 81, 102, 94, 107, 203 по модулю 13,

г) чисел 57, 115, 138, 69, 107 по модулю 12,

д) чисел 41, 87, 105, 13, 127 по модулю 14,

е) чисел 77, 91, 138, 121, 101 по модулю 17.

15. Найти количество натуральных чисел, меньших чисел:

а) 101, б) 131, в) 270, г) 341, д) 600 и взаимно простых с ними.

16. Найти количество натуральных чисел, не превышающих числа:

а) 103, б) 144, в) 152, г) 160, д) 720 и взаимно простых с ним.

17. Показать, что:

а) $1^{16}+3^{16}+7^{16}+9^{16}\equiv 4 \pmod{10}$,

б) $1^{14}+5^{14}+7^{14}+11^{14}\equiv 4 \pmod{12}$,

в) $1^{11}+2^{11}+4^{11}+5^{11}+7^{11}+8^{11}\equiv 0 \pmod{9}$,

г) $1^{17}+3^{17}+5^{17}+9^{17}+11^{17}+13^{17}\equiv 0 \pmod{14}$,

д) $1^{13}+5^{13}+7^{13}+11^{13}\equiv 0 \pmod{12}$.

18. Найти остаток от деления:

а) числа 11^{1201} на число 1000,

в) числа 7^{1199} на число 1000,

в) числа 3^{157} на число 100.

19. Найти число, составленное тремя цифрами младших разрядов числа 3^{798}.

20. Найти две последние цифры чисел:

а) 17^{61}, б) 19^{79}, в) 7^{114}, г) 11^{203}, д) 7^{302}.

21. Исходя из представления данного числа N в виде $N=10a+b$, где a — количество десятков, b — цифра единиц числа N, вывести признаки делимости числа N на числа:

а) 7, б) 13, в) 39, г) 59.

22. Используя соответствующие признаки делимости, установить делимость

а) числа 9633 на число 39,

б) числа 8918 на число 7,

в) числа 29148 на число 7,

г) числа 7493 на число 59,

д) числа 9633 на число 13.

§ 2. СРАВНЕНИЯ С НЕИЗВЕСТНОЙ ВЕЛИЧИНОЙ

Ш. Х. Михелович. Теория чисел, стр. 61—68, 82—86, 87—94, 98—115.

А. А. Бухштаб. Теория чисел, стр. 106—114, 120—123, 126—131, 135—139.

Вопросы для самопроверки

1. Дано сравнение $ax \equiv b \pmod{m}$. При каких условиях оно имеет единственное решение, не имеет решений, имеет $\alpha > 1$ решений?

2. Какие вы знаете методы решения сравнений первой степени?

3. Напишите формулы решения сравнения

$$ax \equiv b \pmod{m}, \text{ где } (a, m) = 1.$$

4. Почему сравнение $f(x) \equiv 0 \pmod{m}$ имеет не больше чем m решений?

5. Почему решения сравнения $f(x) \equiv 0 \pmod{m}$ достаточно искать среди чисел 0, 1, 2, ..., $m-1$?

6. Дайте определение квадратичного вычета и невычета по данному модулю.

7. Сформулируйте закон взаимности.

8. Перечислите свойства символа Лежандра.

9. В чем заключается необходимое и достаточное условие того, чтобы сравнение $f(x) \equiv 0 \pmod{p}$ имело максимальное число решений?

10. Сформулируйте критерий Эйлера для квадратичных вычетов и квадратичных невычетов.

11. Дано сравнение $f(x) \equiv 0 \pmod{p}$, где $f(x)$ — многочлен степени $n \geqslant p$. Как понизить степень этого сравнения, не нарушая эквивалентности сравнения?

12. При каких условиях сравнение $f(x) \equiv 0 \pmod{p}$ удовлетворяется тождественно?

13. При каких условиях многочлен n-й степени может быть разложен по простому модулю на n различных линейных множителей?

Разберите решения следующих примеров.

Пример 1. Решить сравнения:

$$\text{а) } 5x \equiv 2 \pmod{8};$$

$$\text{б) } 7x \equiv 2 \pmod{13}.$$

Решение. а) Так как $(5, 8) = 1$, то сравнение имеет единственное решение. Найдем его с помощью формулы

$$x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

Тогда

$$x \equiv 2 \cdot 5^{\varphi(8)-1} \pmod 8,$$

$$x \equiv 2 \cdot 5^3 = 250 \equiv 2 \pmod 8.$$

Ответ: $x \equiv 2 \pmod 8$.

б) Так как $(7, 13) = 1$, то сравнение

$$7x \equiv 2 \pmod{13},$$

имеет единственное решение.

Решим это сравнение методом проб, основанным на свойстве полной системы вычетов, заставляя x в форме $7x$ пробегать последовательно значения 0, 1, 2, ..., 12.

Устанавливаем, что значения x, равные 0, 1, 2, 3, не удовлетворяют данному сравнению. При $x=4$ имеем:

$$(7 \cdot 4 - 2) \vdots 13,$$

а следовательно, $x=4$ есть решение данного сравнения. Так как сравнение имеет единственное решение, то процесс нахождения решения закончен. Сравнению удовлетворяет целый класс чисел по данному модулю; следовательно, решение сравнения получаем в виде:

$$x \equiv 4 \pmod{13}.$$

Замечание. Отметим, что метод решения сравнения, основанный на применении теоремы Эйлера и малой теоремы Ферма, нельзя отнести к рациональным методам решения сравнений.

В ряде упражнений результат может быть получен быстрее, если использовать искусственный прием, основанный на следующем свойстве сравнения: к любой части сравнения можно прибавить число, кратное модулю. Поясним это на примерах.

а) $5x \equiv 2 \pmod 8$.

Прибавим к правой части сравнения число 8, равное модулю, получим:

$$5x \equiv 10 \pmod 8;$$

деля обе части сравнения на число 5, взаимно простое с модулем 8, приходим к результату:

$$x \equiv 2 \pmod 8.$$

б) $7x \equiv 2 \pmod{13}$.

Прибавим к правой части число $26=13\cdot 2$, имеем:

$$7x\equiv 28 \pmod{13}.$$

Так как $(7, 13)=1$, то после деления обеих частей сравнения на 7 получаем:

$$x\equiv 4 \pmod{13}.$$

Пример 2. Решить сравнение $115x\equiv 85 \pmod{355}$.

Решение. Так как $(115, 355)=5$ и 85 делится на 5, то данное сравнение имеет 5 решений.

Сокращаем обе части сравнения и модуль на 5:

$$23x\equiv 17 \pmod{71}.$$

Полученное сравнение имеет единственное решение:

$$x\equiv 10 \pmod{71},$$

так как

$$23x\equiv 230 \pmod{71}.$$

Следовательно, данное сравнение имеет следующие решения:

$$x\equiv 10 \pmod{355},$$
$$x\equiv 81 \pmod{355},$$
$$x\equiv 152 \pmod{355},$$
$$x\equiv 223 \pmod{355},$$
$$x\equiv 294 \pmod{355}.$$

Пример 3. Найти числа, которые при делении на 7, 13, 17 дают в остатке соответственно 4, 9 и 1.

Решение. Искомые числа должны удовлетворить системе сравнений:

$$\begin{cases} x\equiv 4 \pmod{7}, & (1)\\ x\equiv 9 \pmod{13}, & (2)\\ x\equiv 1 \pmod{17}. & (3) \end{cases}$$

Так как модули сравнений попарно взаимно просты, то эта система имеет единственное решение по модулю $M=7\cdot 13\cdot 17$.

Первое сравнение имеет единственное решение:

$$x=7t+4.$$

Подставим в сравнение (2) вместо x выражение $7t+4$. Получим:

$$7t+4\equiv 9 \pmod{13},$$
$$7t\equiv 5 \pmod{13}.$$

Так как $(7, 13)=1$, то последнее сравнение имеет единственное решение $t\equiv 10 \pmod{13}$, т. е. $t=10+13u$. Откуда $x=7(10+13u)+4=91u+74$.

Найдем те значения u, при которых x будет удовлетворять и сравнению (3).

Имеем: $91u+74\equiv 1 \pmod{17}$ или $6u\equiv 12 \pmod{17}$. Откуда $u\equiv 2 \pmod{17}$, следовательно, $u=2+17k$. Итак, $x=91(2+17k)+74=256+1547k$ или $x\equiv 256 \pmod{1547}$.

Пример 4. Решить систему сравнений:

$$\begin{cases} 3x\equiv 5 \pmod 7, \\ 2x\equiv 3 \pmod 5, \\ 3x\equiv 3 \pmod 9. \end{cases}$$

Решение. Так как модули данных сравнений попарно взаимно простые числа, то данная система имеет решение по модулю, являющемуся произведением данных модулей, т. е. по модулю 315. Обращаясь к коэффициентам при неизвестном и соответствующим модулям, для первого сравнения имеем $(3, 7)=1$, для второго $(2, 5)=1$, для третьего $(3, 9)=3$ и, таким образом, первое и второе сравнения имеют единственное решение, третье сравнение — 3 решения. Легко установить, что решение данной системы сводится к решению трех систем:

$$\begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 4 \pmod 5, \\ x\equiv 1 \pmod 9; \end{cases} \quad \begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 4 \pmod 5, \\ x\equiv 4 \pmod 9; \end{cases} \quad \begin{cases} x\equiv 4 \pmod 7, \\ x\equiv 4 \pmod 5, \\ x\equiv 7 \pmod 9. \end{cases}$$

Далее можно найти все решения данной системы, решая каждую из полученных трех систем сравнений (см. решение предыдущего примера). Получим нижеследующие решения:

$$x\equiv 4 \pmod{315}, \quad x\equiv 109 \pmod{315}, \quad x\equiv 214 \pmod{315}.$$

Решение данной системы может быть осуществлено значительно проще, а именно: решая первое и второе из данных сравнений, получим:

$$x\equiv 4 \pmod 7, \; x\equiv 4 \pmod 5.$$

Замечая, что левые и правые части сравнений одинаковы, воспользуемся свойством: если сравнение имеет место по нескольким модулям, то это сравнение имеет место по модулю, являющемуся наименьшим общим кратным дан-

ных модулей, т. е. система двух рассматриваемых сравнений равносильна сравнению

$$x \equiv 4 \pmod{35}.$$

Далее можно, найдя решение третьего сравнения

$$x \equiv 1 \pmod 9, \quad x \equiv 4 \pmod 9, \quad x \equiv 7 \pmod 9,$$

перейти к нижеследующим системам:

$$\begin{cases} x \equiv 4 \pmod{35}, \\ x \equiv 1 \pmod 9; \end{cases} \quad \begin{cases} x \equiv 4 \pmod{35}, \\ x \equiv 4 \pmod 9; \end{cases} \quad \begin{cases} x \equiv 4 \pmod{35}, \\ x \equiv 7 \pmod 9. \end{cases}$$

Решение каждой из этих систем не вызывает затруднений. Заметим, что система сравнений

$$\begin{cases} x \equiv 4 \pmod{35}, \\ x \equiv 4 \pmod 9 \end{cases}$$

сразу дает решение

$$x \equiv 4 \pmod{315}.$$

Можно поступить иначе: к выше полученному решению первых двух сравнений в виде

$$x \equiv 4 \pmod{35},$$

присоединим третье из данных сравнений

$$3x \equiv 3 \pmod 9$$

и, заметив, что искомое решение данной системы должно быть получено по модулю 315, последовательно будем иметь:

$$x = 35k + 4, \quad 3(35k + 4) \equiv 3 \pmod 9, \quad 105k \equiv 0 \pmod 9,$$
$$6k \equiv 0 \pmod 9.$$

Последнее сравнение имеет три решения по модулю 9, а именно:

$$k \equiv 0 \pmod 9, \quad k \equiv 3 \pmod 9, \quad k \equiv 6 \pmod 9.$$

Получаем

$$x = 35 \cdot 9u + 4 = 315u + 4,$$
$$x = 35(9u + 3) + 4 = 315u + 109,$$
$$x = 35(9u + 6) + 4 = 315u + 214,$$

или соответственно

$$x \equiv 4 \pmod{315}, \quad x \equiv 109 \pmod{315}, \quad x \equiv 214 \pmod{315}.$$

Остановимся еще на одном приеме решения системы сравнений.

Пример 5. Решить систему сравнений:

$$\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 7 \pmod{25}. \end{cases}$$

Решение. Заметим, что данные модули, т. е. числа 15 и 25, не являются взаимно простыми. В этом случае следует сначала убедиться в существовании решений.

Если дана система сравнений:

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \end{cases}$$

где $(m_1, m_2) = \alpha > 1$, то эта система будет иметь решение при условии:

$$c_1 \equiv c_2 \pmod{\alpha}.$$

Обращаясь к данной системе сравнений, имеем: $(15, 25) = 5$, $2 \equiv 7 \pmod 5$, т. е. данная система совместна.

Из первого сравнения получаем:

$$x = 15t + 2;$$

подставив это значение x во второе сравнение, приходим к сравнению

$$15t + 2 \equiv 7 \pmod{25},$$

т. е.

$$15t \equiv 5 \pmod{25}.$$

После сокращения обеих частей сравнения и модуля на 5 получим:

$$\begin{gathered} 3t \equiv 1 \pmod 5, \\ 3t \equiv 6 \pmod 5, \\ t \equiv 2 \pmod 5, \\ t = 5k + 2; \end{gathered}$$

теперь нахождение решения данной системы сравнений не вызывает затруднений:

$$\begin{gathered} x = 15t + 2 = 15(5k + 2) + 2 = 75k + 32, \\ x \equiv 32 \pmod{75}. \end{gathered}$$

Найденное решение является единственным, что вытекает из единственности решения каждого из сравнений данной системы.

Правильность полученного решения может быть легко проверена его подстановкой в каждое из сравнений данной системы.

Замечание. Рассмотрим прием решения, который, на наш взгляд, является рациональным в целом ряде случаев.

Дана система сравнений:

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1}, \\ a_2x \equiv b_2 \pmod{m_2}, \end{cases} \tag{1}$$

где $(m_1, m_2) = (a_1, m_1) = (a_2, m_2) = 1$. Эту систему заменим эквивалентной ей системой:

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \end{cases} \tag{2}$$

где первое и второе из сравнений системы (2) являются соответственно решениями первого и второго сравнений системы (1).

От системы (2) перейдем к системе

$$\begin{cases} m_2x \equiv m_2c_1 \pmod{m_1 \cdot m_2}, \\ m_1x \equiv m_1c_2 \pmod{m_1 \cdot m_2}. \end{cases} \tag{3}$$

Покажем эквивалентность системы сравнений (2) и системы сравнений (3).

Пусть x_1 — любое решение системы сравнений (2) по модулю $m_1 \cdot m_2$. Тогда справедлива следующая система сравнений:

$$\begin{cases} x_1 \equiv c_1 \pmod{m_1}, \\ x_1 \equiv c_2 \pmod{m_2}, \end{cases}$$

которая после умножения обеих частей сравнений и модулей соответственно на m_2 и m_1 приводит к справедливым сравнениям:

$$\begin{cases} m_2x_1 \equiv m_2c_1 \pmod{m_1 \cdot m_2}, \\ m_1x_1 \equiv m_1c_2 \pmod{m_1 \cdot m_2}, \end{cases}$$

откуда x_1 — решение системы сравнений (3) по модулю $m_1 \cdot m_2$. Обратно, если x_2 — любое решение системы сравнений (3) по модулю $m_1 \cdot m_2$, то справедлива следующая система сравнений:

$$\begin{cases} m_2x_2 \equiv m_2c_1 \pmod{m_1 \cdot m_2}, \\ m_1x_2 \equiv m_1c_2 \pmod{m_1 \cdot m_2}. \end{cases}$$

Следовательно,

$$\begin{cases} x_2 \equiv c_1 \pmod{m_1}, \\ x_2 \equiv c_2 \pmod{m_2} \end{cases}$$

и x_2 — решение системы сравнений (2) по модулю $m_1 m_2$.

Таким образом, системы сравнений (2) и (3) эквивалентны, а так как система сравнений (2) имеет единственное решение по модулю $m_1 \cdot m_2$, то и система сравнений (3) тоже имеет единственное решение.

При решении системы сравнений рассмотренным способом в случае попарно взаимно простых модулей нет необходимости заменять систему (1) системой (2).

Пример. Решить систему сравнений:

$$\begin{cases} 3x \equiv 5 \pmod 7, \\ 2x \equiv 1 \pmod 5. \end{cases}$$

Решение: Так как $(3, 7) = (2, 5) = 1$, то каждое из сравнений имеет единственное решение; $(7, 5) = 1$ и, следовательно, данная система имеет единственное решение по модулю 35.

От данной системы переходим к системе сравнений

$$\begin{cases} 15x \equiv 25 \pmod{35}, \\ 14x \equiv 7 \pmod{35} \end{cases}$$

и, вычитая из первого сравнения второе, получаем искомое решение:

$$x \equiv 18 \pmod{35}.$$

Применим рассмотренный прием к некоторым решенным выше упражнениям.

Пример. Решить систему сравнений:

$$\begin{cases} 3x \equiv 5 \pmod 7, \\ 2x \equiv 3 \pmod 5, \\ 3x \equiv 3 \pmod 9. \end{cases}$$

Решение. Как установлено выше, система совместна и имеет три решения по модулю 315. Получаем систему:

$$\begin{cases} 135x \equiv 225 \pmod{315}, \\ 126x \equiv 189 \pmod{315}, \\ 105x \equiv 105 \pmod{315}. \end{cases}$$

Первые два сравнения дают

$$9x \equiv 36 \pmod{315}.$$

Умножая обе части сравнения на 11, где $(11, 315) = 1$, имеем:

$$99x \equiv 396 \pmod{315}.$$

Вычитая полученное сравнение из сравнения

$$105x \equiv 105 \pmod{315},$$

приходим к сравнению:

$$6x \equiv 24 \pmod{315},$$

а так как $(2, 315) = 1$, то получаем:

$$3x \equiv 12 \pmod{315}.$$

Искомые решения:

$$x \equiv 4 \pmod{315},\ x \equiv 109 \pmod{315},\ x \equiv 214 \pmod{315}.$$

Пример. Решить систему сравнений:

$$\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 7 \pmod{25}. \end{cases}$$

Решение. Выше установлено, что данная система имеет единственное решение по модулю 75.

Переходим к системе сравнений:

$$\begin{cases} 5x \equiv 10 \pmod{75}, \\ 3x \equiv 21 \pmod{75}, \end{cases}$$

откуда

$$\begin{aligned} 2x &\equiv -11 \pmod{75}, \\ 2x &\equiv 64 \pmod{75}, \end{aligned}$$

так как $(2, 75) = 1$, то

$$x \equiv 32 \pmod{75}$$

является искомым решением.

Пример 6. Решить сравнение $17x \equiv 7 \pmod{30}$.

Решение. Модулем сравнения является составное число 30, каноническим разложением которого будет: $30 = 2 \cdot 3 \cdot 5$. Следовательно, решение данного сравнения можно свести к решению системы:

$$\begin{cases} 17x \equiv 7 \pmod{2}, \\ 17x \equiv 7 \pmod{3}, \\ 17x \equiv 7 \pmod{5}. \end{cases} \qquad (1)$$

Система сравнений (1) эквивалентна следующей системе:

$$\begin{cases} x \equiv 1 \pmod 2, \\ 2x \equiv 1 \pmod 3, \\ x \equiv 1 \pmod 5. \end{cases}$$

Решение последней системы предлагаем найти читателю. Решением будет $x \equiv 11 \pmod{30}$. Рекомендуем читателю решить данное сравнение, не сводя его к системе сравнений.

Пример 7. С помощью критерия Эйлера среди чисел 3, 5, 7 и 9 найти квадратичные вычеты по модулю 13.

Решение. Замечаем, что каждое из данных чисел взаимно просто с модулем, а поэтому критерий Эйлера применим.

Как известно, если $(a, p) = 1$ и $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, то a — квадратичный вычет по модулю p.

В данном примере имеем:

$$3^6 = (27)^2 \equiv 1 \pmod{13};$$
$$5^6 = (25)^3 \equiv (-1)^3 \equiv -1 \pmod{13};$$
$$7^6 = (49)^3 \equiv (-3)^3 \equiv -1 \pmod{13};$$
$$9^6 \equiv (-4)^6 \equiv 16^3 \equiv 3^3 \equiv 1 \pmod{13}.$$

Итак, числа 3 и 9 являются квадратичными вычетами, а 5 и 7 — квадратичными невычетами по модулю 13.

Пример 8. Показать, что нечетное число, взаимно простое с числом 10, возведенное в тридцатую степень, может оканчиваться лишь цифрами 1 и 9.

Решение. Если x — искомое число, то решение сведется к нахождению числа a в качестве наименьшего неотрицательного вычета по модулю 10 в сравнении

$$x^{30} \equiv a \pmod{10},$$

где $(x, 10) = 1$ (по условию задачи), $(a, 10) = 1$ (по свойству сравнений).

Так как $(x, 10) = 1$, $\varphi(10) = 4$, то на основании теоремы Эйлера справедливо сравнение

$$x^4 \equiv 1 \pmod{10}.$$

Возведя обе части сравнения в седьмую степень, получим сравнение:

$$x^{28} \equiv 1 \pmod{10}.$$

На основании последнего сравнения и сравнения

$$x^{30} \equiv a \pmod{10}$$

приходим к сравнению

$$x^2 \equiv a \pmod{10}, \text{ где } (a, 10) = 1.$$

Остается найти квадратичные вычеты по модулю 10, которыми являются числа 1, 9, в чем можно убедиться, проверив, что из сравнений

$$x^2 \equiv 1 \pmod{10},$$
$$x^2 \equiv 9 \pmod{10},$$
$$x^2 \equiv 3 \pmod{10},$$
$$x^2 \equiv 7 \pmod{10}$$

только первые два имеют решения соответственно:

$$x \equiv 1;\ 9 \pmod{10},$$
$$x \equiv 3;\ 7 \pmod{10}.$$

Пример 9. Решить сравнение:

$$5x^2 + x - 4 \equiv 0 \pmod{11}.$$

Решение. Умножим обе части сравнения на число 20, где $(20, 11) = 1$. Получим сравнение:

$$100x^2 + 20x - 80 \equiv 0 \pmod{11},$$

или

$$(10x+1)^2 \equiv 81 \pmod{11}.$$

Обозначим $10x+1$ через z. Итак $z^2 \equiv 81 \pmod{11}$, или $z^2 \equiv 4 \pmod{11}$.

Решим это сравнение методом проб. Испытывая числа 0, 1, 2, ..., 10, видим, что сравнение имеет решения: $z=2$ и $z=9$, т. е. удовлетворяется при $z=2+11t$ и $z=9+11t$.

Так как $z=10x+1$, то $x=\frac{z-1}{10}$, т. е.

$$x_1 = \frac{11t+1}{10}, \quad x_2 = \frac{11t+8}{10};$$

при $t=9$ имеем $x_1=10$ и при $t=2$ получаем $x_2=3$.

Следовательно, данное сравнение имеет решения 3 и 10, т. е. ему удовлетворяют целые числа вида: $x=3+11t$, $x=10+11t$.

Ответ:

$$x \equiv 3 \pmod{11},$$
$$x \equiv 10 \pmod{11}.$$

Замечание. Придя к необходимости решения сравнения

$$z^2 \equiv 81 \pmod{11},$$

получаем очевидное решение $z \equiv 9 \pmod{11}$, а на основании одного из свойств двучленных сравнений получаем второе решение $z \equiv 11-9 \pmod{11}$, т. е. $z \equiv 2 \pmod{11}$. Далее, как указано выше.

Пример 10. С помощью символа Лежандра установить, имеет ли решение сравнение: $x^2 \equiv 22 \pmod{13}$.

Решение. Если символ Лежандра $\left(\frac{a}{p}\right) = 1$, то сравнение $x^2 \equiv a \pmod{p}$ имеет два решения, а если $\left(\frac{a}{p}\right) = -1$, то сравнение решений не имеет.

Таким образом, решение сведется к вычислению символа Лежандра $\left(\frac{22}{13}\right)$. Воспользуемся свойством: если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, следовательно, $\left(\frac{22}{13}\right) = \left(\frac{9}{13}\right)$; далее воспользуемся свойством $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$, откуда $\left(\frac{9}{13}\right) = \left(\frac{3^2}{13}\right) = 1$.

Так как $\left(\frac{22}{13}\right) = 1$, то сравнение $x^2 \equiv 22 \pmod{13}$ имеет два решения.

Применение искусственных приемов позволяет в отдельных случаях не только ответить на вопрос о существовании решений сравнения, но и найти эти решения, если они существуют.

Пример 11. Имеет ли решение сравнение:

$$x^2 \equiv 19 \pmod{31}?$$

Решение. К правой части сравнения прибавим число 62, кратное модулю, получим:

$$x^2 \equiv 81 \pmod{31}.$$

Отсюда $x \equiv 9 \pmod{31}$ и $x \equiv 22 \pmod{31}$.

Рассмотрим аналогичный способ решения 10-го примера.

$$x^2 \equiv 22 \pmod{13},$$
$$x^2 \equiv 9 \pmod{13}.$$

Следовательно, $x \equiv 3 \pmod{13}$, $x \equiv 10 \pmod{13}$.

Пример 12. Решить сравнение:

$$x^7-3x^6+x^5-x^3+4x^2-4x+2\equiv 0 \pmod 5.$$

Решение. Так как степень сравнения $n>p$, где p — модуль сравнения, то данное сравнение можно заменить эквивалентным ему сравнением, степень которого меньше модуля сравнения. Для этого многочлен

$$x^7-3x^6+x^5-x^3+4x^2-4x+2$$

разделим на x^5-x; в остатке получим многочлен

$$x^2-3x+2.$$

Следовательно, данное сравнение эквивалентно сравнению

$$x^2-3x+2\equiv 0 \pmod 5.$$

Методом проб легко показать, что это сравнение имеет два решения:

$$x\equiv 1 \pmod 5,\ x\equiv 2 \pmod 5.$$

Замечание. Сравнение $x^2-3x+2\equiv 0 \pmod 5$ можно представить в виде $(x-1)\cdot(x-2)\equiv 0 \pmod 5$, откуда $x\equiv 1 \pmod 5$, $x\equiv 2 \pmod 5$.

Пример 13. Сравнение $7x^4-9x^3+8x^2+10x-6\equiv 0 \pmod{11}$ заменить равносильным ему сравнением со старшим коэффициентом, равным единице.

Решение. Так как старший коэффициент данного сравнения равен 7 и $(7, 11)=1$, то находим единственное решение сравнения $7a\equiv 1 \pmod{11}$ в виде $a\equiv 8 \pmod{11}$.

Учитывая, что $(8, 11)=1$, умножим обе части исходного сравнения на число 8, не меняя модуля сравнения, и получим

$$56x^4-72x^3+64x^2+80x-48\equiv 0 \pmod{11}.$$

После ряда упрощений приходим к сравнению

$$x^4+5x^3-2x^2+3x-4\equiv 0 \pmod{11},$$

которое равносильно данному.

Этот же пример может быть решен иначе. Заменив коэффициенты данного сравнения числами, сравнимыми с ними по модулю 11, но меньшими по абсолютной величине, получим:

$$-4x^4+2x^3-3x^2-x+5\equiv 0 \pmod{11}.$$

Умножим обе части сравнения на —3, не меняя модуля, так как число —3 взаимно просто с модулем, что вытекает из следующих соотношений: $-3 \equiv 8 \pmod{11}$, $(8, 11) = 1$. Получим сравнение:

$$12x^4 - 6x^3 + 9x^2 + 3x - 15 \equiv 0 \pmod{11},$$

равносильное данному.

После упрощения приходим к сравнению

$$x^4 + 5x^3 - 2x^2 + 3x - 4 \equiv 0 \pmod{11}.$$

Пример 14. Разложить многочлен

$$f(x) = x^4 + 7x^3 + x - 9$$

на множители по модулю 13.

Решение. Рассмотрим сравнение:

$$x^4 + 7x^3 + x - 9 \equiv 0 \pmod{13}.$$

Легко заметить, что оно имеет решение

$$x \equiv 1 \pmod{13},$$

а поэтому справедливо тождественное сравнение

$$x^4 + 7x^3 + x - 9 \equiv (x-1)(x^3 + 8x^2 + 8x + 9) \pmod{13}.$$

Далее рассмотрим сравнение

$$x^3 + 8x^2 + 8x + 9 \equiv 0 \pmod{13}.$$

Оно также имеет решение $x \equiv 1 \pmod{13}$, а поэтому

$$x^4 + 7x^3 + x - 9 \equiv (x-1)^2 (x^2 + 9x + 17) \pmod{13},$$

или

$$x^4 + 7x^3 + x - 9 \equiv (x-1)^2 (x^2 - 4x + 4) \pmod{13}.$$

Следовательно, искомое разложение имеет вид:

$$x^4 + 7x^3 + x - 9 \equiv (x-1)^2 (x-2)^2 \pmod{13}.$$

Пример 15. Разложить многочлен

$$f(x) = x^4 - 4x^2 + x + 2$$

на множители по модулю 7.

Решение. Рассмотрим сравнение

$$x^4 - 4x^2 + x + 2 \equiv 0 \pmod{7}.$$

Легко установить, что это сравнение имеет нижеследующие решения:

$$x \equiv 1 \pmod{7}, \quad x \equiv -2 \pmod{7}.$$

Применяя схему Горнера,

	1	0	—4	1	2
1	1	1	—3	—2	0
—2	1	—1	—1	0	

получим:

$$(x-1)(x+2)(x^2-x-1)\equiv 0 \pmod 7.$$

Остается либо попытаться найти решения сравнения

$$x^2-x-1\equiv 0 \pmod 7,$$

либо установить, что последнее сравнение не имеет решений.

Можно было бы, например, пойти по пути проверки значений полной системы вычетов по модулю 7, применяя схему Горнера.

Мы выберем другой путь и прежде всего выясним, имеет это сравнение решения или нет.

Преобразуем сравнение

$$x^2-x-1\equiv 0 \pmod 7.$$

Последовательно получим:

$$x^2+6x-1\equiv 0 \pmod 7,$$
$$(x+3)^2\equiv 3 \pmod 7.$$

Положим $x+3=z$, откуда

$$z^2\equiv 3 \pmod 7.$$

Применяя свойства символа Лежандра, получим:

$\left(\frac{3}{7}\right)=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1$ и соответственно сравнение $x^2-x-1\equiv 0 \pmod 7$ не имеет решений.

Окончательно получаем следующее разложение данного многочлена

$$(x-1)(x+2)(x^2-x-1)\equiv 0 \pmod 7.$$

Пример 16. Выяснить, имеет ли сравнение

$$3x^3-x^2+4x+1\equiv 0 \pmod 7$$

три решения.

Решение. Данное сравнение имеет три решения, если при делении x^7-x на левую часть сравнения получим остаток, коэффициенты которого кратны модулю. Предварительно данное сравнение заменим эквивалентным ему сравнением со старшим коэффициентом, равным единице (см. решение примера 13). Получим сравнение

$$x^3+2x^2-x-2\equiv 0 \pmod 7.$$

Остается найти остаток от деления x^7-x на x^3+2x^2-x-2 и убедиться, что коэффициенты остатка кратны модулю.

Замечание. В отдельных случаях удается не только ответить на поставленный вопрос, но одновременно найти и решения сравнения. Так в данном примере имеем:

$$\begin{gathered} x^3+2x^2-x-2\equiv 0 \pmod 7, \\ x(x^2-1)+2(x^2-1)\equiv 0 \pmod 7, \\ (x^2-1)(x+2)\equiv 0 \pmod 7, \\ (x-1)(x+1)(x+2)\equiv 0 \pmod 7, \end{gathered}$$

следовательно, $x\equiv 1 \pmod 7$, $x\equiv -1 \pmod 7$, $x\equiv -2 \pmod 7$ — решения данного сравнения.

Пример 17. Найти однозначное положительное число, 27-я степень которого оканчивается цифрой 7.

Решение. Если обозначим искомое число через x, то для нахождения его потребуется решить сравнение

$$x^{27}\equiv 7 \pmod{10},$$

где $(7, 10)=1$.

По одному из свойств сравнения

$$a\equiv b \pmod m,$$

$(b, m)=(a, m)$, отсюда $(x, 10)=1$. Применив теорему Эйлера, получим сравнение

$$x^4\equiv 1 \pmod{10},$$

так как $\varphi(10)=4$. Возведем обе части последнего сравнения в 6-ю степень, после чего придем к сравнению

$$x^{24}\equiv 1 \pmod{10}.$$

Тогда сравнение

$$x^{27}\equiv 7 \pmod{10}$$

можно преобразовать следующим образом:

$$\begin{gathered} x^{27}=x^{24}\cdot x^3\equiv x^3 \pmod{10}, \\ x^3\equiv 7 \pmod{10}. \end{gathered}$$

Так как $(x, 10)=1$, то, проверяя подстановкой в последнее сравнение числа 1, 3, 5, 7, 9, находим единственное решение $x\equiv 3 \pmod{10}$. Следовательно,

$$3^{27}\equiv 7 \pmod{10}.$$

Пример 18. Решить сравнение

$$x^2\equiv 1 \pmod{16}.$$

Решение. Используем метод проб, подвергая проверке числа, взаимно простые с модулем, так как $(1, 16)=1$, т. е. числа 1, 3, 5, 7, 9, 11, 13, 15. Искомые решения:

$$x\equiv 1 \pmod{16},\ x\equiv 7 \pmod{16},\ x\equiv 9 \pmod{16},$$
$$x\equiv 15 \pmod{16}.$$

Это подтверждает положение, что если модуль — составное число, то сравнение степени n по этому модулю может иметь более n решений.

Пример 19. Показать, что если a — нечетное число, то для того чтобы сравнение

$$x^2\equiv a \pmod{8}$$

имело решения, необходимо и достаточно выполнение условия:

$$a\equiv 1 \pmod{8}.$$

Решение. Условие необходимости. Пусть

$$x\equiv x_0 \pmod{8}$$

есть решение данного сравнения, тогда

$$x_0^2\equiv a \pmod{8},$$

так как $(a, 8)=1$, то x_0 — нечетное число, общий вид которого $4k\pm 1$. Легко видеть, что

$$(4k\pm 1)^2\equiv 1 \pmod{8}.$$

откуда $a\equiv 1 \pmod{8}$.

Условие достаточности. Если $a\equiv 1 \pmod{8}$, то данное сравнение равносильно сравнению

$$x^2\equiv 1 \pmod{8},$$

которому удовлетворяет любое нечетное число, и данное сравнение имеет решения.

Пример 20. Показать, что произведение двух квадратичных вычетов по простому модулю есть квадратич-

ный вычет по тому же модулю, а произведение квадратичного вычета на невычет есть квадратичный невычет по тому же простому модулю.

Решение. Если a и b — квадратичные вычеты по модулю p, то на основании критерия Эйлера:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

$$b^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Перемножая эти сравнения, имеем:

$$(a \cdot b)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

и ab — квадратичный вычет по модулю p. Во втором случае

$$(ab)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

и ab — квадратичный невычет по модулю p.

Пример 21. Доказать, что для символа Лежандра справедливо свойство

$$\left(\frac{q}{p}^{n}\right) = \left(\frac{q}{p}\right)^{n}.$$

Решение. На основании одного из свойств символа Лежандра справедливо:

$$\left(\frac{a \cdot b \cdot c \cdot \ldots \cdot k}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \cdot \left(\frac{c}{p}\right) \cdot \ldots \cdot \left(\frac{k}{p}\right).$$

Остается положить

$$a = b = c = \ldots = k = q,$$

считая количество сомножителей в числителе символа Лежандра равным n.

Упражнения

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) $5x \equiv 3 \pmod{17}$;
ж) $3x \equiv 5 \pmod{11}$;
з) $9x \equiv 2 \pmod{14}$;
и) $10x \equiv 15 \pmod{25}$;
к) $9x \equiv 12 \pmod{21}$;
л) $28x \equiv 40 \pmod{44}$;
м) $24x \equiv 14 \pmod{26}$;
н) $21x \equiv 33 \pmod{45}$;
о) $30x \equiv 18 \pmod{102}$;
п) $21x \equiv 35 \pmod{77}$.

2. Решить системы сравнений:

а) $\begin{cases} x \equiv 3 \pmod{11}, \\ x \equiv 5 \pmod{7}; \end{cases}$

б) $\begin{cases} x \equiv 6 \pmod{7}, \\ x \equiv 2 \pmod{13}; \end{cases}$

в) $\begin{cases} x \equiv 3 \pmod{17}, \\ 3x \equiv 6 \pmod{9}; \end{cases}$

г) $\begin{cases} x \equiv 7 \pmod{11}, \\ x \equiv 3 \pmod{10}, \\ x \equiv 2 \pmod{3}; \end{cases}$

д) $\begin{cases} 7x \equiv 10 \pmod{11}, \\ 12x \equiv 7 \pmod{13}, \\ 7x \equiv 11 \pmod{15}; \end{cases}$

е) $\begin{cases} x \equiv 13 \pmod{16}, \\ x \equiv 3 \pmod{10}, \\ x \equiv 9 \pmod{14}; \end{cases}$

ж) $\begin{cases} x \equiv 4 \pmod{15}, \\ x \equiv 1 \pmod{12}, \\ x \equiv 7 \pmod{14}. \end{cases}$

3. Найти числа, которые при делении на 13, 5 и 12 дают соответственно в остатке 5, 1 и 7.

4. Найти числа, которые при делении на 7, 11 и 13 дают соответственно в остатке 3, 2 и 5.

5. Найти числа, которые при делении на 7, 11 и 17 дают соответственно в остатке 3, 5 и 13.

6. С помощью критерия Эйлера установить, какие из чисел 3, 5, 7, 8 являются квадратичными вычетами по модулю 13.

7. С помощью критерия Эйлера установить, какие из чисел 5, 6, 7, 8 являются квадратичными невычетами по модулю 11.

8. С помощью критерия Эйлера установить, имеют ли решения сравнения:

а) $x^2 \equiv 3 \pmod{7}$;
б) $x^2 \equiv 5 \pmod{11}$;
в) $x^2 \equiv 6 \pmod{13}$;
г) $x^2 \equiv 5 \pmod{7}$;
д) $x^2 \equiv 7 \pmod{11}$;
е) $x^2 \equiv 12 \pmod{13}$.

9. С помощью символа Лежандра установить, имеют ли решения сравнения:

а) $x^2 \equiv 404 \pmod{523}$;
б) $x^2 \equiv 99 \pmod{601}$;
в) $x^2 \equiv 219 \pmod{383}$;
г) $x^2 \equiv 47 \pmod{73}$;
д) $x^2 \equiv 231 \pmod{101}$;
е) $x^2 \equiv 33 \pmod{179}$;
ж) $x^2 \equiv 65 \pmod{193}$;
з) $x^2 \equiv 26 \pmod{241}$;
и) $x^2 \equiv 30 \pmod{269}$;
к) $x^2 \equiv 42 \pmod{251}$.

10. Простейшим способом найти решения сравнений:

а) $x^2 \equiv 20 \pmod{101}$;
б) $x^2 \equiv 6 \pmod{47}$;
в) $x^2 \equiv 7 \pmod{59}$;
г) $x^2 \equiv 12 \pmod{23}$;
д) $x^2 \equiv 7 \pmod{31}$.

11. Заменить данные сравнения равносильными им сравнениями, степени которых ниже p, где p— модуль:

а) $x^8-3x^7+2x^6+3x^4-2x^2-1\equiv 0 \pmod 5$;
б) $x^{13}-x^3+x-3\equiv 0 \pmod{11}$;
в) $x^8-2x^7+3x^6+x^5-2x^2-x-3\equiv 0 \pmod 5$;
г) $x^9-3x^4+2x^3-x+3\equiv 0 \pmod 7$;
д) $x^{10}+3x^5-4x^3+x^2-3\equiv 0 \pmod 7$;
е) $x^{14}-x^{12}+3x^5-6x^2+x+1\equiv 0 \pmod{11}$.

12. Решить следующие сравнения:

а) $x^8-x^6+x^5-x^4+2x^2-x+3\equiv 0 \pmod 5$;
б) $x^9-x^3+x-5\equiv 0 \pmod 7$;
в) $x^8-x^4+2x-3\equiv 0 \pmod 5$;
г) $x^{12}+2x^{11}-2x-1\equiv 0 \pmod{11}$;
д) $x^{14}-4x^{13}-x+6\equiv 0 \pmod{13}$.

13. Сравнения:

а) $7x^5-2x^4+5x^3-x^2+3x-2\equiv 0 \pmod{11}$;
б) $11x^3-6x^2+2x-5\equiv 0 \pmod{15}$;
в) $2x^5-4x^4+3x^3-2x+3\equiv 0 \pmod{13}$;
г) $3x^6-2x^5+3x^3+2x^2-3\equiv 0 \pmod 7$;
д) $5x^4-3x^3+2x^2-x+5\equiv 0 \pmod{11}$

заменить равносильными им сравнениями со старшими коэффициентами, равными единице.

14. Разложить на множители:
а) многочлен x^3-8x^2-x+3 по модулю 11,
б) многочлен x^4-3x^2-x+4 по модулю 7,
в) многочлен x^4-4x^3+4x-1 по модулю 7,
г) многочлен $x^4+6x^3-3x^2+x+2$ по модулю 13,
д) многочлен x^3+2 по модулю 5.

15. Имеет ли сравнение

$$x^3+3x-1\equiv 0 \pmod 5,$$

три различных решения?

16. Имеет ли сравнение

$$x^4-5x^2-3\equiv 0 \pmod 7$$

четыре различных решения?

17. Имеет ли сравнение

$$x^2+3\equiv 0 \pmod 7$$

два различных решения?

Ш. Х. Михелович. Теория чисел, стр. 125—146.
А. А. Бухштаб. Теория чисел, стр. 139—167.

Вопросы для самопроверки

1. Дайте определение показателя, которому принадлежит число a по модулю m.
2. На основании какой теоремы можно утверждать, что всякое число a, взаимно простое с модулем m, принадлежит тому или иному показателю?
3. Сколько существует различных показателей, которым могут принадлежать числа по модулю m?
4. Дайте определение первообразного корня по данному модулю m.
5. Какому показателю принадлежит число a— первообразный корень по простому модулю m?
6. Сколько существует первообразных корней по простому модулю p?
7. Сформулируйте признак первообразного корня по простому модулю p.
8. Для какого вида чисел существуют первообразные корни по составному модулю?
9. Дайте определение индекса числа по простому модулю.
10. Сформулируйте основные свойства индексов.

Разберите решения следующих примеров:

Пример 1. Какому показателю принадлежит число 5 по модулю 12?

Решение. Должны быть выполнены следующие требования:

а) число, принадлежащее показателю, должно быть взаимно простым с модулем;

б) искомый показатель надо искать среди делителей числа $\varphi(m)$, где m — модуль;

в) искомый показатель должен быть наименьшим из положительных показателей, удовлетворяющих сравнению $a^z \equiv 1 \pmod{m}$, где a — испытуемое число.

В данном случае имеем:

$$(5,\ 12)=1;\ \varphi(12)=12\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)=4;$$

делителями 4 являются числа 1, 2, 4; получим:

$$5\equiv 5\pmod{12},\ 5^2\equiv 1\pmod{12},$$

следовательно, число 5 принадлежит показателю 2 по модулю 12.

Пример 2. Какому показателю принадлежит число 4 по модулю 12?

Решение. В данном случае нарушено одно из требований определения; числа 4 и 12 не являются взаимно простыми, а следовательно, сама постановка вопроса является ошибочной.

Пример 3. Зная, что число 2 есть первообразный корень по модулю 37, показать справедливость сравнения

$$2^{18}\equiv 6^2\pmod{37}.$$

Решение. На основании малой теоремы Ферма справедливо сравнение

$$2^{36}\equiv 1\pmod{37},$$

или

$$(2^{18}+1)(2^{18}-1)\equiv 0\pmod{37},$$

откуда

$$(2^{18}+1)(2^{18}-1)\ \vdots\ 37.$$

Так как 2 — первообразный корень по данному модулю, то

$$(2^{18}-1)\ \text{не}\ \vdots\ 37$$

и справедливо сравнение:

$$2^{18}+1\equiv 0\pmod{37},$$
$$2^{18}\equiv -1\pmod{37}.$$

Прибавляя к правой части сравнения число 37, равное модулю, имеем:

$$2^{18}\equiv 36\pmod{37},$$
$$2^{18}\equiv 6^2\pmod{37}.$$

Пример 4. Найти наименьший первообразный корень по модулю 7.

Решение. Для нахождения наименьшего первообразного корня по простому модулю p необходимо и достаточно:

а) найти все различные простые делители числа $p-1$ (обозначим их $p_1, p_2, \ldots, p_k$);

б) последовательно проверить числа, взаимно простые с модулем, начиная с числа 1; первое из чисел, которое не удовлетворяет ни одному из сравнений:

$$q^{\frac{p-1}{p_1}} \equiv 1 \pmod{p}, \ldots, q^{\frac{p-1}{p_k}} \equiv 1 \pmod{p}$$

будет искомым первообразным корнем.

Имеем $7-1=6=2\cdot 3$; таким образом, q будет первообразным корнем, если не имеет место ни одно из сравнений:

$$q^3 \equiv 1 \pmod 7, \quad q^2 \equiv 1 \pmod 7.$$

Так как

$$1^2 \equiv 1 \pmod 7.$$

то число 1 не является первообразным корнем по модулю 7;

$2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$, и число 2 не является первообразным корнем по модулю 7;

$3^2 \equiv 2 \pmod 7$, $3^3 \equiv -1 \pmod 7$, следовательно, число 3 — наименьший первообразный корень по модулю 7.

Пример 5. Показать, что составное число 4 имеет первообразные корни.

Решение. Надо показать, что по крайней мере одно из чисел, взаимно простых с модулем m, принадлежит показателю $\varphi(m)$.

Возьмем сравнение

$$a^z \equiv 1 \pmod m, \text{ где } (a, m) = 1.$$

Для данного примера имеем: $a^z \equiv 1 \pmod 4$. Находим $\varphi(4)=2$. Так как $(3, 4)=1$, то проверяем число 3, получаем $3^1 \equiv 3 \pmod 4$, $3^2 \equiv 1 \pmod 4$, т. е. число 3 — первообразный корень по модулю 4.

Пример 6. Показать, что не существует первообразных корней по модулю 8.

Решение. Представителями классов чисел, взаимно простых с модулем, возьмем числа 1, 3, 5, 7: так как $\varphi(8)=4$, то показателями, которым могут принадлежать эти числа, являются делители числа 4, т. е. 1, 2, 4.

Имеем: $1^1 \equiv 1 \pmod 8$, т. е. 1 принадлежит показателю единица, остальные числа принадлежат показателю 2, так как

$$3^2 \equiv 1 \pmod 8,$$
$$5^2 \equiv (-3)^2 \equiv 1 \pmod 8,$$
$$7^2 \equiv (-1)^2 \equiv 1 \pmod 8$$

и первообразных корней по модулю 8 не существует.

Приведем более изящное решение. Любое нечетное число, а только нечетные числа взаимно просты с модулем $8=2^3$, может быть представлено в виде:

$$a=4n\pm 1;$$

возводя обе части в квадрат, получим:

$$a^2=2^4n^2\pm 2^3n+1,$$

откуда

$$a^2 \equiv 1 \pmod 8.$$

Так как

$$\varphi(8)=4,$$

то, следовательно, не существует первообразных корней по модулю 8.

Пример 7. Найти наименьший из первообразных корней по модулю 37 и составить таблицу индексов, приняв этот корень за основание индексов; составить таблицу для нахождения числа по данному индексу.

Решение. Находим наименьший первообразный корень по модулю 37 (см. решение примера 4).

Устанавливаем, что искомым корнем является число 2. Это число принимаем за основание индексов. Находим наименьшие положительные вычеты по модулю 37, заставляя x пробегать последовательно значения от 0 до 35. Имеем:

$2^0 \equiv 1$	$2^8 \equiv 34$	$2^{16} \equiv 9$	$2^{24} \equiv 10$	$2^{32} \equiv 7$
$2^1 \equiv 2$	$2^9 \equiv 31$	$2^{17} \equiv 18$	$2^{25} \equiv 20$	$2^{33} \equiv 14$
$2^2 \equiv 4$	$2^{10} \equiv 25$	$2^{18} \equiv 36$	$2^{26} \equiv 3$	$2^{34} \equiv 28$
$2^3 \equiv 8$	$2^{11} \equiv 13$	$2^{19} \equiv 35$	$2^{27} \equiv 6$	$2^{35} \equiv 19$
$2^4 \equiv 16$	$2^{12} \equiv 26$	$2^{20} \equiv 33$	$2^{28} \equiv 12$	
$2^5 \equiv 32$	$2^{13} \equiv 15$	$2^{21} \equiv 29$	$2^{29} \equiv 24$	
$2^6 \equiv 27$	$2^{14} \equiv 30$	$2^{22} \equiv 21$	$2^{30} \equiv 11$	
$2^7 \equiv 17$	$2^{15} \equiv 23$	$2^{23} \equiv 5$	$2^{31} \equiv 22$	

Таблица

для нахождения по данному числу соответствующего ему индекса

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

Таблица

для нахождения по данному индексу соответствующего ему числа

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Замечание. В учебниках и учебных пособиях можно встретить таблицы индексов, составленные по различным первообразным корням для одного и того же простого числа, что не влияет на ответы упражнений, предложенных ниже.

Пример 8. Найти число решений сравнений:

$$\text{а) } x^{15}\equiv 6 \pmod{37},$$
$$\text{б) } 3x^3\equiv 2 \pmod{37}.$$

Решение. Модуль данных сравнений является простым числом.

а) Берем индексы от обеих частей сравнения

$$x^{15}\equiv 6 \pmod{37}$$

и получаем сравнение

$$15\operatorname{ind} x\equiv \operatorname{ind} 6 \pmod{36}.$$

Так как $\text{ind}\ 6 \equiv 27 \pmod{36}$, то сравнение принимает вид:

$$15\,\text{ind}\ x \equiv 27 \pmod{36}.$$

Это сравнение первой степени относительно $\text{ind}\ x$, и замечая, что $(15, 36) = 3$ и $27 \vdots 3$, устанавливаем, что данное сравнение имеет 3 решения.

б) Взяв индексы от обеих частей сравнения, получим сравнение:

$$\text{ind}\ 3 + 3\,\text{ind}\ x \equiv \text{ind}\ 2 \pmod{36},$$
$$3\,\text{ind}\ x \equiv \text{ind}\ 2 - \text{ind}\ 3 \pmod{36};$$

по таблице индексов находим:

$$\text{ind}\ 2 \equiv 1 \pmod{36},\quad \text{ind}\ 3 \equiv 26 \pmod{36}.$$

После соответствующей замены сравнение принимает вид:

$$3\,\text{ind}\ x \equiv 1 - 26 \pmod{36},$$
$$3\,\text{ind}\ x \equiv 11 \pmod{36}.$$

Так как $(3, 36) = 3$, 11 не $\vdots$ 3, то это сравнение, а следовательно, и данное сравнение не имеют решений.

Пример 9. С помощью таблицы индексов решить сравнение

$$13x^3 \equiv 24 \pmod{37}.$$

Решение. Берем индексы от обеих частей сравнения и, используя свойства индексов, имеем:

$$\text{ind}\ 13 + 3\,\text{ind}\ x \equiv \text{ind}\ 24 \pmod{36}.$$

Из таблицы индексов (первой) для простого числа 37 находим:

$$\text{ind}\ 13 \equiv 11 \pmod{36},\ \text{ind}\ 24 \equiv 29 \pmod{36}.$$

(Таблицы взяты из книги Ш. Х. Михеловича. Теория чисел.)

Следовательно, $11 + 3\,\text{ind}\ x \equiv 29 \pmod{36}$,

$$3\,\text{ind}\ x \equiv 18 \pmod{36}.$$

Так как $(3, 36) = 3$ и $18 \vdots 3$, то сравнение имеет три решения; после упрощения имеем: $\text{ind}\ x \equiv 6 \pmod{12}$, откуда $\text{ind}\ x_1 \equiv 6 \pmod{36}$, $\text{ind}\ x_2 \equiv 18 \pmod{36}$, $\text{ind}\ x_3 \equiv 30 \pmod{36}$, (см. решение сравнений первой степени);

по таблице индексов (для нахождения числа по данному индексу) находим:

$$x_1 \equiv 27 \pmod{37},\ x_2 \equiv 36 \pmod{37},\ x_3 \equiv 11 \pmod{37},$$

являющиеся решениями данного сравнения.

Пример 10. Решить сравнение:

$$21^{3x} \equiv 21^5 \pmod{29}.$$

Решение. Берем индексы от обеих частей сравнения и, используя свойства индексов, получаем:

$$3x \operatorname{ind} 21 \equiv 5 \operatorname{ind} 21 \pmod{28};$$

по таблице индексов находим:

$$\operatorname{ind} 21 \equiv 17 \pmod{28}$$

и сравнение принимает вид:

$$17(3x-5) \equiv 0 \pmod{28}.$$

Так как $(17, 28) = 1$, то приходим к условию

$$(3x-5) \vdots 28,$$

которое эквивалентно сравнению

$$3x \equiv 5 \pmod{28},$$

решение которого

$$x \equiv 11 \pmod{28}.$$

Рассмотрим другой способ решения. Воспользуемся следующим свойством: если g — первообразный корень по модулю p и

$$g^k \equiv g^l \pmod{p},$$

то

$$k \equiv l \pmod{p-1}.$$

Установив, что 21 — первообразный корень по модулю 29, приходим к решению сравнения

$$3x \equiv 5 \pmod{28},$$

откуда

$$x \equiv 11 \pmod{28}.$$

Пример 11. Найти все первообразные корни по модулю 17; записать их в виде наименьших положительных вычетов.

Решение. Задача может быть решена различными приемами. Рассмотрим их.

1. Можно использовать прием, посредством которого решен пример 4.

2. Находим наименьший первообразный корень по модулю 17 (см. решение примера 4), который равен 3; заметим, что если число g принадлежит показателю $p-1$, где p — модуль, то этому же показателю будут принадлежать числа вида g^k, если $(k, p-1)=1$ и $1<k<p-1$. Выписываем числа 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15; среди них взаимно простые с числом 16 числа 3, 5, 7, 9, 11, 13, 15; вычислим остальные первообразные корни в форме наименьших положительных вычетов по модулю 17:

$$3^3 \equiv 10 \pmod{17},$$
$$3^5 \equiv 3^2 \cdot 10 \equiv 5 \pmod{17},$$
$$3^7 \equiv 3^5 \cdot 3^2 \equiv 5 \cdot 9 \equiv 11 \pmod{17},$$
$$3^9 \equiv 10 \cdot 5 \cdot 3 \equiv -3 \equiv 14 \pmod{17},$$
$$3^{11} \equiv 14 \cdot 9 \equiv -3 \cdot 9 \equiv 7 \pmod{17},$$
$$3^{13} \equiv 7 \cdot 9 \equiv 12 \pmod{17},$$
$$3^{15} \equiv 12 \cdot 9 \equiv (-5) \cdot 9 \equiv 6 \pmod{17}.$$

Таким образом, первообразными корнями по модулю 17 являются числа 3, 5, 6, 7, 10, 11, 12, 14.

Пример 12. С помощью таблиц индексов найти показатель, которому принадлежит число 13 по модулю 79.

Решение. $(13, 79)=1$, а поэтому искомый показатель должен удовлетворять сравнению $13^\delta \equiv 1 \pmod{79}$.

Применяя свойство индексов, имеем:

$$\delta \operatorname{ind} 13 \equiv \operatorname{ind} 1 \pmod{78}.$$

Пользуясь таблицей индексов, находим:

$$\operatorname{ind} 13 \equiv 34 \pmod{78}, \quad \operatorname{ind} 1 \equiv 0 \pmod{78},$$

и сравнение принимает вид:

$$34\delta \equiv 0 \pmod{78},$$
$$17\delta \equiv 0 \pmod{39};$$

наименьшее положительное значение $\delta=39$, удовлетворяющее этому сравнению, будет являться искомым показателем.

Пример 13. Пользуясь таблицей индексов, распределить числа по показателям по простому модулю 7.

Решение. Возьмем сравнение:

$$a^{\delta} \equiv 1 \pmod 7,$$

где $(a, 7) = 1$. Замечая, что число 1 принадлежит показателю 1, ограничимся значениями

$$a = 2, 3, 4, 5, 6.$$

Беря индексы от обеих частей сравнения, имеем:

$$\delta \operatorname{ind} a \equiv 0 \pmod 6,$$

и надо найти наименьшее положительное δ, удовлетворяющее условию

$$\delta \operatorname{ind} a \vdots 6.$$

По таблице индексов находим:

$$\operatorname{ind} 2 \equiv 2 \pmod 6, \ \operatorname{ind} 3 \equiv 1 \pmod 6,$$
$$\operatorname{ind} 4 \equiv 4 \pmod 6, \ \operatorname{ind} 5 \equiv 5 \pmod 6, \ \operatorname{ind} 6 \equiv 3 \pmod 6.$$

Так, если $a=2$, то условие принимает вид: $\delta \cdot 2 \vdots 6$, откуда $\delta = 3$. Аналогично находим: $1 \cdot \delta \vdots 6$, $\delta = 6$, и число 3 принадлежит показателю 6 (первообразный корень по модулю 7); $4\delta \vdots 6$, $\delta = 3$, и число 4 принадлежит показателю 3; $5\delta \vdots 6$, $\delta = 6$, и число 5 принадлежит показателю 6 (первообразный корень по модулю 7); $3\delta \vdots 6$, $\delta = 2$, и число 6 принадлежит показателю 2 по модулю 7.

Пример 14. Зная, что число 5 есть первообразный корень по модулю 7, найти, каким показателям принадлежат числа 5^2, 5^3, 5^4 по тому же модулю.

Решение. Так как число 5, являясь первообразным корнем по модулю 7, принадлежит показателю 6, то для решения поставленной задачи достаточно найти частное от деления числа 6 на наибольший общий делитель числа 6 и показателя степени испытуемого числа. Таким образом, для числа 5^2 имеем: $\frac{6}{(6, 2)} = 3$, аналогично для числа 5^3 получим: $\frac{6}{(6, 3)} = 2$, наконец, для числа 5^4 — $\frac{6}{(6, 4)} = 3$.

Следовательно, данные числа принадлежат соответственно показателям 3; 2; 3.

Пример 15. Доказать, что первообразный корень g по простому модулю p есть квадратичный невычет по тому же модулю.

Решение. Из определения первообразного корня следует, что число g принадлежит показателю $p-1$ по модулю p.

Напишем сравнение:

$$g^{p-1} \equiv 1 \pmod{p}, \text{ где } p \geq 2,$$

и, преобразовав сравнение, получим:

$$(g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p},$$

откуда

$$(g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \vdots p.$$

Так как g — первообразный корень, то сравнение

$$g^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

невозможно и, следовательно,

$$g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}, \; g^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

следовательно, g — квадратичный невычет по модулю p.

Пример 16. Число 43 — первообразный корень по модулю 89; показать, что сравнение

$$x^2 \equiv 43 \pmod{89}$$

не имеет решений.

Решение. На основании предыдущего упражнения устанавливаем, что число 43 — квадратичный невычет по модулю 89, и, следовательно, сравнение $x^2 \equiv 43 \pmod{89}$ не имеет решений.

Пример 17. Показать, что среди первообразных корней по простому модулю $p > 2$ не может быть полных квадратов.

Решение. Допустим, что это не так и первообразный корень $g = k^2$. Тогда сравнение

$$x^2 \equiv k^2 \pmod{p}$$

имеет очевидное решение

$$x \equiv k \pmod{p},$$

откуда $g = k^2$ — квадратичный вычет по модулю p, т. е. приходим к сравнению

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

что невозможно, так как g — первообразный корень.

Упражнения

1. Какому показателю принадлежат:

а) число 2 по модулю 5,
б) число 3 по модулю 7,
в) число 5 по модулю 8,
г) число 7 по модулю 10,
д) число 5 по модулю 11,
е) число 6 по модулю 13,
ж) число 7 по модулю 15,
з) число 3 по модулю 17.

2. Найти все показатели, которым принадлежат числа:

а) по модулю 7,
б) по модулю 8,
в) по модулю 9,
г) по модулю 10,
д) по модулю 11,
е) по модулю 12,
ж) по модулю 13,
з) по модулю 15.

3. Распределить классы чисел по показателям:

а) по модулю 5, в) по модулю 7, д) по модулю 9,
б) по модулю 6, г) по модулю 8, е) по модулю 10.

4. Найти наименьший первообразный корень:

а) по модулю 11, г) по модулю 19, ж) по модулю 41,
б) по модулю 13, д) по модулю 23, з) по модулю 43,
в) по модулю 17, е) по модулю 29, и) по модулю 47.

5. Составить таблицу индексов:

а) по модулю 11, б) по модулю 19, в) по модулю 29

6. Решить сравнения:

а) $25^x \equiv 32 \pmod{59}$,
б) $13^x \equiv 24 \pmod{53}$,
в) $12^{x^2} \equiv 17 \pmod{47}$,
г) $3^{x^2} \equiv 23 \pmod{29}$.

7. Определить число решений сравнений:

а) $x^{15} \equiv 6 \pmod{37}$,
б) $x^3 \equiv 2 \pmod{37}$.

8. С помощью таблиц индексов решить сравнения:

а) $43x^{17} \equiv 65 \pmod{79}$,
б) $13x^4 \equiv 17 \pmod{37}$,
в) $17x^4 \equiv 19 \pmod{73}$,
г) $23x^3 \equiv 58 \pmod{97}$,
д) $2x^6 \equiv 5 \pmod{31}$,
е) $3x^5 \equiv 16 \pmod{31}$,

ж) $7x^3 \equiv 14 \pmod{41}$,
з) $2x^4 \equiv 33 \pmod{43}$,
и) $5x^3 \equiv 38 \pmod{47}$.

9. Найти все первообразные корни:

а) по модулю 13,
б) по модулю 19,
в) по модулю 23,
г) по модулю 29,
д) по модулю 31,
е) по модулю 41.

10. С помощью таблиц индексов найти показатели, которым принадлежат:

а) число 5 по модулю 17,
б) число 7 по модулю 19,
в) число 11 по модулю 23,
г) число 13 по модулю 29,
д) число 8 по модулю 31,
е) число 10 по модулю 37,
ж) число 17 по модулю 41,
з) число 19 по модулю 43,
и) число 15 по модулю 47,
к) число 23 по модулю 53.

§ 4. АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

Ш. Х. Михелович Теория чисел, стр. 147—160.
А. А. Бухштаб. Теория чисел, стр. 201—209.

Вопросы для самопроверки

1. На каких свойствах сравнения основано нахождение остатка при делении на данное число?
2. Сформулируйте свойства сравнений, на которых основаны выводы признаков делимости.
3. Чему равна длина периода (число цифр в периоде) чистой периодической дроби?
4. Сколько цифр между целой частью числа и первым периодом смешанной периодической дроби?
5. Получено $236 \cdot 421 = 99\,536$. Чем вызвано, что проверка с помощью числа 9 не обнаруживает ошибки, допущенной в результате действия?

Разберите решения следующих примеров:

Пример 1. Найти остаток от деления числа 20^{6n+5} на число 9, где n — целое неотрицательное число.

Решение. Замечая, что на основании метода сравнений можно вычитать и прибавлять к любой части срав-

нений числа, кратные модулю (это относится и к основанию степени), рассмотрим два случая, а именно:

а) $n=0$, тогда имеем:

$$20^5 \equiv 2^5 = 2^3 \cdot 2^2 \equiv (-1) \cdot 2^2 \equiv 5 \pmod 9,$$

б) $n \neq 0$, тогда последовательно имеем:

$$20^{6n+5} \equiv 2^{6n+5} = (2^3)^{2n} \cdot 2^5 \equiv (-1)^{2n} \cdot 5 \equiv 5 \pmod 9.$$

Искомый остаток равен 5.

Пример 2. Показать, что при любом целом неотрицательном n число $3 \cdot 5^{2n+1} + 2^{3n+1}$ делится на число 17.

Решение. Как и в предыдущем примере рассмотрим два случая:

а) если $n=0$, то очевидно число 17 делится на 17;

б) если $n \neq 0$, то последовательно имеем:

$$3 \cdot 5^{2n+1} + 2^{3n+1} = 3 \cdot 5 \cdot (5^2)^n + 2^{3n+1} \equiv$$
$$\equiv (-2)(5^2)^n + 2^{3n+1} \equiv (-2)(2^3)^n + 2^{3n+1} \equiv 0 \pmod{17},$$

т. е. данное число делится на 17.

Пример 3. Пользуясь основными свойствами сравнений, найти остаток от деления $125 \cdot 465$ на 61.

Решение. Легко заметить, что

$$125 \equiv 3 \pmod{61}; \quad 465 \equiv 38 \pmod{61}.$$

Перемножим почленно эти сравнения. Получим, что

$$125 \cdot 465 \equiv 38 \cdot 3 \pmod{61},$$

т. е.

$$125 \cdot 465 \equiv 53 \pmod{61}.$$

Итак, искомый остаток равен 53.

Пример 4. Показать, что число $13^{176}-1$ делится на 89.

Решение. $13^{176}-1 = (13^{88}-1)(13^{88}+1)$; 89 — число простое, а поэтому на основании малой теоремы Ферма

$$13^{88} \equiv 1 \pmod{89},$$

т. е. $(13^{88}-1) \vdots 89$. Следовательно, $(13^{176}-1) \vdots 89$.

Пример 5. Показать, что число $14^{120}-1$ делится на 45.

Решение. $(14, 45) = 1$, а поэтому на основании теоремы Эйлера

$$14^{\varphi(45)} \equiv 1 \pmod{45},$$

т. е. $14^{24} \equiv 1 \pmod{45}$, так как $\varphi(45) = 24$.

Возведем последнее сравнение почленно в пятую степень. Тогда

$$14^{120} \equiv 1 \pmod{45}.$$

Это значит, что $14^{120}-1$ делится на 45.

Пример 6. Найти последние две цифры числа 5^{100}.

Решение. Найти последние две цифры числа — это значит найти остаток, полученный при делении этого числа на 100.

$$5^{100} = 25^{50} = 625^{25} \equiv 25^{25} = 25 \cdot 625^{12} \equiv$$
$$\equiv 25 \cdot 25^{12} = 25 \cdot 625^{6} \equiv 25 \cdot 25^{6} = 25 \cdot 625^{3} \equiv$$
$$\equiv 25 \cdot 25^{3} \equiv 25^{2} \equiv 25 \pmod{100}.$$

Итак, искомый остаток есть 25. Следовательно, последними двумя цифрами числа 5^{100} будут: 2 (десятки) и 5 (единицы).

Пример 7. С помощью таблиц индексов найти остаток от деления 10^{10} на 67.

Решение. Обозначим искомый остаток через r, т. е.

$$10^{10} \equiv r \pmod{67}.$$

Берем индексы от обеих частей сравнения:

$$10 \operatorname{ind} 10 \equiv \operatorname{ind} r \pmod{66}.$$

Из первой таблицы индексов для простого числа 67 находим, что $\operatorname{ind} 10 \equiv 16 \pmod{66}$, следовательно, $160 \equiv \operatorname{ind} r \pmod{66}$, или $\operatorname{ind} r \equiv 28 \pmod{66}$. Теперь из второй таблицы индексов находим, что

$$r \equiv 23 \pmod{67}.$$

Итак, искомый остаток равен 23.

Замечание. Выше дан один из методов обоснования признаков делимости чисел. Рассмотрим второй метод, основанный на свойстве сравнений. Если

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

многочлен с целыми коэффициентами, где $a_n \not\equiv 0 \pmod{m}$, $x \equiv y \pmod{m}$, то $f(x) \equiv f(y) \pmod{m}$.

Поставим перед собой задачу в процессе обоснования использовать либо сравнение $10^k \equiv 1 \pmod{d}$, либо сравнение $10^k \equiv -1 \pmod{d}$ (см. ниже), где k — целое поло-

жительное число, d — целое положительное число, о делимости на которое идет речь.

Пример 8. Установить признаки делимости на число 11.

Решение. Рассмотрим некоторые из признаков.

1. Данное число N представим в виде

$$N=a_0+a_1\cdot 10+a_2\cdot 10^2+a_3\cdot 10^3+\ldots,$$

где $0\leqslant a_i\leqslant 9$, $d=11$. Справедливо сравнение

$$10\equiv -1 \pmod{11}.$$

Приходим к сравнению

$$N\equiv a_0-a_1+a_2-a_3+\ldots \pmod{11}.$$

Воспользуемся свойством: если

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

то $(a,\ m)=(b,\ m)$, следовательно, если $N \vdots 11$, то $(a_0-a_1+a_2-a_3+\ldots) \vdots 11$, и обратно. Полученный признак делимости можно сформулировать в следующей форме: число N делится на число 11 тогда и только тогда, когда разность между суммой цифр числа N, стоящих на нечетных местах, и суммой цифр того же числа, стоящих на четных местах, делится на 11.

2. Замечая, что $1001=11\cdot 7\cdot 13$, представим:

$$N=a_0+a_1\cdot 10^3+a_2(10^3)^2+a_3(10^3)^3+\ldots,$$

где $0\leqslant a_i\leqslant 999$, $d=11$. Справедливо

$$10^3\equiv -1 \pmod{1001}.$$

Приходим к сравнению

$$N\equiv a_0-a_1+a_2-a_3+\ldots \pmod{1001}.$$

Согласно одному из свойств сравнение, имеющее место по некоторому модулю, справедливо и по модулю, являющемуся положительным делителем данного модуля. Получаем:

$$N\equiv a_0-a_1+a_2-a_3+\ldots \pmod{11}.$$

Справедливость этого признака можно обосновать так же, как и в предыдущем примере, но можно выбрать и иной путь: из последнего сравнения следует, что

$$[N-(a_0-a_1+a_2-a_3+\ldots)] \vdots 11.$$

Известно, что если разность и уменьшаемое делятся на 11, то и вычитаемое делится на 11. А так же, если разность и вычитаемое делятся на 11, то и уменьшаемое делится на 11.

Теперь можно сформулировать соответствующий признак делимости: разбиваем число N на грани справа налево по три цифры в каждой грани; число N делится на число 11 тогда и только тогда, когда разность между суммой чисел, стоящих в четных гранях, и суммой чисел, стоящих в нечетных гранях, делится на 11.

Заметим, что признаки делимости на 7 и 13 аналогичны признакам делимости на 11. Для доказательства достаточно повторить все рассуждения, заменив число 11 соответственно числами 7 и 13.

Пример 9. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичную дробь обыкновенной дроби $\frac{13}{17}$.

Решение. $(10, 17) = 1$, а поэтому длина периода периодической дроби равна δ, где δ есть показатель, которому принадлежит число 10 по модулю 17. Найдем δ.

Для этой цели воспользуемся таблицей индексов для простого числа 17. Число δ должно удовлетворять сравнению

$$10^{\delta} \equiv 1 \pmod{17}.$$

Берем индексы от обеих частей сравнения:

$$\delta \operatorname{ind} 10 \equiv \operatorname{ind} 1 \pmod{16},$$

или

$$3\delta \equiv 0 \pmod{16}.$$

Наименьшее положительное число, удовлетворяющее этому сравнению, будет число 16. Следовательно, $\delta = 16$.

Пример 10. Найти длину периода и число цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная дробь $\frac{17}{220}$.

Решение. Каноническим разложением числа 220 будет $2^2 \cdot 5 \cdot 11$. Так как $(11, 10) = 1$, то для нахождения длины периода найдем показатель δ, которому принадлежит 10 по модулю 11:

$$10 \equiv -1 \pmod{11},$$
$$10^2 \equiv 1 \pmod{11}.$$

Следовательно, $\delta=2$.

Число цифр λ между запятой и первым периодом равно наибольшему показателю, с которым входят сомножители 2 и 5 в каноническое разложение знаменателя данной дроби.

Следовательно, $\lambda=2$.

Пример 11. Проверить результаты действий с помощью числа 9:

а) $24667+18265=42932$;

б) $5433153:4371=1243$.

Решение. а) Суммы цифр слагаемых соответственно равны 25 и 22; сумма цифр суммы — 20. Легко заметить, что $25+22\equiv 20 \pmod 9$.

Следовательно, в первом примере можно полагать, что сложение выполнено правильно.

б) Во втором примере суммы цифр делителя и частного соответственно равны 15 и 10; сумма цифр делимого 24. Так как $24\equiv 150 \pmod 9$, то можно полагать, что деление выполнено правильно.

Пример 12. Показать, что остаток от деления числа $3^{19\cdot 37-1}$ на $19\cdot 37$ равен 1.

Решение. Достаточно показать, что справедливо сравнение

$$3^{19\cdot 37-1}\equiv 1 \pmod{19\cdot 37}.$$

Преобразуем показатель степени:

$$19\cdot 37-1=(18+1)(36+1)-1=18\cdot 36+54.$$

Так как $(19, 37)=1$, то

$$\varphi(19\cdot 37)=\varphi(19)\cdot\varphi(37)=18\cdot 36.$$

На основании теоремы Эйлера

$$3^{18\cdot 36}\equiv 1 \pmod{19\cdot 37},$$

где $(3, 19\cdot 37)=1$.

С другой стороны, имеем:

$$3^{19\cdot 37-1}=3^{18\cdot 36}\cdot 3^{54}\equiv 3^{54} \pmod{19\cdot 37}.$$

На основании малой теоремы Ферма $3^{18}\equiv 1 \pmod{19}$, где $(3, 19)=1$. Непосредственным вычислением легко установить, что $3^{18}\equiv 1 \pmod{37}$ (см. решение примера 1).

На основании свойства, по которому из сравнимости двух чисел по нескольким модулям вытекает их сравни-

мость по модулю, являющемуся наименьшим общим кратным исходных модулей, имеем:

$$3^{18} \equiv 1 \pmod{19 \cdot 37}.$$

Возведя обе части сравнения в третью степень, получим:

$$3^{54} \equiv 1 \pmod{19 \cdot 37}.$$

Итак,

$$3^{19 \cdot 37 - 1} \equiv 1 \pmod{19 \cdot 37}.$$

Упражнения

1. Найти остаток от деления числа 48^{5n+3} на 11, где n — любое целое неотрицательное число.

2. Найти остаток от деления числа 48^{5n+4} на 11, где n — любое целое неотрицательное число.

3. Показать, что при любом целом неотрицательном n число $7 \cdot 3^{3n+1} - 2^{3n+1}$ делится на 19.

4. Показать, что при любом целом неотрицательном n число $25 \cdot 7^{2n} + 2^{3n+4}$ делится на 41.

5. Показать, что при любом целом неотрицательном n число $11 \cdot 3^{5n} + 2 \cdot 13^{2n+1}$ делится на 37.

6. Найти две цифры младших разрядов чисел:

а) 5^{40}, б) 6^{32}, в) 8^{18}, г) 3^{12}, д) 2^{33}, е) 4^{20}.

7. Найти остаток от деления чисел:

а) 11^{802}, б) 13^{1602}, в) 7^{1203}, г) 17^{2001}, д) 19^{2402} на число 1000.

8. Вывести и сформулировать признак делимости на число 11, исходя из сравнения

$$10^2 \equiv 1 \pmod{99};$$

проиллюстрировать применение признака двумя числовыми примерами.

9. Вывести и сформулировать признак делимости на число 33, исходя из сравнения

$$10^2 \equiv 1 \pmod{99};$$

проиллюстрировать применение признака двумя числовыми примерами.

10. Вывести и сформулировать признаки делимости на числа 27 и 37, учитывая, что

$$999 = 27 \cdot 37,$$

и используя сравнение

$$10^3 \equiv 1 \pmod{999};$$

проиллюстрировать применение признака двумя числовыми примерами.

11. Используя соответствующий признак делимости, проверить делимость чисел:

а) 3038035, 3138135, 3539635 на число 11;
б) 4735731, 4739735 на число 11;
в) 3138135, 4735731 на число 33;
г) 559013, 3038035 и 3138135 на число 13;
д) 3038035 и 3539635 на число 65;
е) 52434, 79974, 111888 на число 27;
ж) 11934, 52434, 111888 на число 54;
з) 121878, 141858, 145854 на число 37;
и) 111888, 121878, 145854 на число 111;
к) 90585 и 254925 на число 165.

12. С помощью таблиц индексов найти остатки от деления:

а) числа $85 \cdot 79$ на число 97,
б) числа $53 \cdot 41 \cdot 17$ на число 59,
в) числа $89 \cdot 78$ на число 61.

13. Используя таблицы индексов найти остатки от деления:

а) числа 13^{19} на число 31,
б) числа 29^{17} на число 41,
в) числа 31^{18} на число 37,
г) числа 17^{19} на число 53,
д) числа 7^{23} на число 59,
е) числа 11^{37} на число 61,
ж) числа 19^{32} на число 67.

14. Используя понятие числа, принадлежащего показателю, найти длину периода при обращении в десятичные дроби обыкновенных несократимых дробей:

а) со знаменателем 7,
б) со знаменателем 11,
в) со знаменателем 13,
г) со знаменателем 23,
д) со знаменателем 29,
е) со знаменателем 31,
ж) со знаменателем 37,
з) со знаменателем 43.

15. Найти длину периода и количество цифр между запятой и периодом десятичной дроби, в которую обращается обыкновенная несократимая дробь:

а) со знаменателем 35,
б) со знаменателем 110,
в) со знаменателем 76,
г) со знаменателем 210,
д) со знаменателем 208,
е) со знаменателем 620,
ж) со знаменателем 85,
з) со знаменателем 860.

16. С помощью числа 9 проверить результат арифметических действий:

а) $24667+18265=42932$,
б) $141811+17128=158932$,
в) $37918-13207=24711$,
г) $42932-18265=24667$,
д) $4371\cdot1243=5433153$,
е) $1042\cdot1011=1053462$,
ж) $421767:3429=123$,
з) $115403365:23845=48417$.

§ 5. НЕПРЕРЫВНЫЕ ДРОБИ

Ш. Х. Михелович. Теория чисел, стр. 69—82, 161—176.

А. А. Бухштаб. Теория чисел, стр. 58—66.

Вопросы для самопроверки

1. Что вы знаете о представлении любого рационального числа непрерывной дробью?
2. Запишите свойства подходящих дробей.
3. Запишите формулу решения сравнения

$$ax\equiv b\pmod m,\ \text{где}\ (a,\ m)=1,$$

основанного на методе подходящих дробей.

Разберите решения нижеследующих примеров.

Пример 1. Разложить рациональное число $\frac{53}{21}$ в цепную (непрерывную) дробь; составить таблицу ее подходящих дробей, найти подходящую дробь второго порядка.

Решение. Находим элементы (неполные частные):

$$\begin{array}{r|l}
53 & 21 \\
-42 & \overline{2} \\
\hline
21 & 11 \\
-11 & \overline{1} \\
\hline
11 & 10 \\
-10 & \overline{1} \\
\hline
10 & 1 \\
-10 & \overline{10} \\
\hline
0 &
\end{array}$$

Следовательно, $\frac{53}{21}=[2, 1, 1, 10]$ — разложение данного рационального числа в конечную цепную дробь.

Для ответа на второй вопрос составим таблицу

k		0	1	2	3
q_k		2	1	1	10
P_k	1	2	3	5	53
Q_k	0	1	1	2	21

В этой таблице k означает порядок подходящей дроби, q_k — элемент порядка k; P_k, Q_k — соответственно числитель и знаменатель подходящей дроби порядка k. Во втором вертикальном столбце таблицы числа 1 и 0 постоянны для любой таблицы; в третьем столбце учтено, что $P_0=q_0$ и $Q_0=1$; вычисление осуществляется по формулам: $P_k=P_{k-1}\cdot q_k+P_{k-2}$, $Q_k=Q_{k-1}q_k—Q_{k-2}$.

Из таблицы следует, что

$$\frac{P_2}{Q_2}=\frac{5}{2}.$$

Пример 2. Разложить рациональное число $\frac{17}{27}$ в цепную дробь; составить таблицу подходящих дробей; найти подходящую дробь четвертого порядка.

Решение. Процесс аналогичен рассмотренному в предыдущем примере. Последовательно получаем:

$$\begin{array}{r|l}
17 & 27 \\
0 & \hline 0
\end{array}$$

$$\begin{array}{r|l}
27 & 17 \\
17 & \hline 1
\end{array}$$

$$\begin{array}{r|l}
17 & 10 \\
10 & \hline 1
\end{array}$$

$$\begin{array}{r|l}
10 & 7 \\
7 & \hline 1
\end{array}$$

$$\begin{array}{r|l}
7 & 3 \\
6 & \hline 2
\end{array}$$

$$\begin{array}{r|l}
3 & 1 \\
3 & \hline 3
\end{array}$$

$$\begin{array}{|l}
\hline 0
\end{array}$$

Следовательно, $\frac{17}{27}=[0, 1, 1, 1, 2, 3]$. Далее следует составить таблицу подходящих дробей, после чего легко найти, что

$$\frac{P_4}{Q_4}=\frac{5}{8}.$$

Пример 3. Разложить рациональное число $-\frac{37}{17}$ в цепную дробь; составить таблицу подходящих дробей; найти подходящую дробь третьего порядка.

Решение. Предварительно заметим, что в соответствии с определением конечной цепной дроби лишь q_0 может быть любым целым числом, а остальные q_i — целые положительные числа.

Найдем элементы соответствующей цепной дроби:

$$
\begin{array}{rr|l}
 & -37 & 17 \\
- & -51 & \hline -3 \\
\hline
 & 17 & 14 \\
- & 14 & \hline 1 \\
\hline
 & 14 & 3 \\
- & 12 & \hline 4 \\
\hline
 & 3 & 2 \\
- & 2 & \hline 1 \\
\hline
 & 2 & 1 \\
- & 2 & \hline 2 \\
\hline
 & 0 &
\end{array}
$$

Следовательно, $-\frac{37}{17} = [-3, 1, 4, 1, 2]$.

Составим таблицу:

k		0	1	2	3	4
q_k		—3	1	4	1	2
P_k	1	—3	—2	—11	—13	—37
Q_k	0	1	1	5	6	17

Откуда

$$\frac{P_3}{Q_3} = -\frac{13}{6}.$$

Пример 4. Решить сравнение

$$23x \equiv 17 \pmod{71}.$$

Решение. $(23, 71) = 1$, поэтому сравнение имеет единственное решение.

Используем аппарат цепных дробей. Для этого разложим в цепную дробь число $\frac{71}{23}$, получим:

$$\frac{71}{23}=[3,\ 11,\ 2].$$

Составим таблицу значений числителя p_k подходящих дробей:

q_k		3	11	2
P_k	1	3	34	71
E_k		1	-1	1

На основании формулы решения сравнений первой степени с одним неизвестным $x\equiv E_nP_{n-1}b\pmod m$, имеем:

$$x\equiv 1\cdot 34\cdot 17\pmod{71},$$

или

$$x\equiv 10\pmod{71}.$$

Пример 5. Решить сравнение $115x\equiv 85\pmod{355}$.

Решение. Так как $(115, 355)=5$ и 85 делится на 5, то данное сравнение имеет 5 решений.

Сократим обе части сравнения и модуль на 5:

$$23x\equiv 17\pmod{71}.$$

Полученное сравнение имеет единственное решение:

$$x\equiv 10\pmod{71}$$

(см. предыдущий пример).

Следовательно, данное сравнение имеет следующие решения:

$$x\equiv 10\pmod{355},$$
$$x\equiv 81\pmod{355},$$
$$x\equiv 152\pmod{355},$$
$$x\equiv 223\pmod{355},$$
$$x\equiv 294\pmod{355}.$$

Пример 6. Решить неопределенное уравнение

$$23x+91y=2.$$

Решение. Так как

$$(23, 91)=1,$$

то уравнение имеет решение в целых числах; учитывая, что 23 — целое положительное число, его можно принять за модуль соответствующего сравнения, в результате чего получим

$$91y \equiv 2 \pmod{23};$$

прибавляя к левой части сравнения число $-92y$, кратное модулю, приходим к сравнению

$$-y \equiv 2 \pmod{23},$$

откуда

$$y \equiv -2 \pmod{23},\ y = 23t - 2;$$

подставив полученное значение y в данное уравнение, после простейших преобразований находим, что

$$x = 8 - 91t.$$

Получили общее решение данного уравнения в виде

$$x = 8 - 91t,\ y = 23t - 2.$$

Замечания 1. Так как второй коэффициент, равный 91, — целое положительное число, то можно исходить из сравнения

$$23x \equiv 2 \pmod{91};$$

последовательно имеем:

$$\begin{gathered} 23x \equiv 184 \pmod{91}; \\ x \equiv 8 \pmod{91}, \\ x = 91t + 8, \\ 23(91t + 8) + 91y = 2, \\ y = -2 - 23t. \end{gathered}$$

2. Если дано уравнение

$$ax + by = c,$$

где $(a, b) = 1$, $b > 0$, то, решая сравнение

$$ax \equiv c \pmod{b},$$

получаем

$$\begin{gathered} x \equiv x_0 \pmod{b}, \\ x = bt + x_0. \end{gathered}$$

Можно найти значение y по формуле

$$y = \frac{c - ax_0}{b} - at.$$

И, полагая

$$\frac{c-ax_0}{b}=y_0,$$

получаем

$$y=y_0-at.$$

Пример 7. Разложить дробь $\frac{58}{77}$ на сумму или разность двух дробей соответственно со знаменателями 7 и 11.

Решение. Из условия получаем:

$$\frac{x}{7}+\frac{y}{11}=\frac{58}{77},$$

откуда $11x+7y=58$; так как $(11, 7)=1$, то уравнение имеет решение в целых числах. Замечая, что 7 — целое положительное число, приходим к сравнению

$$11x\equiv 58 \pmod 7$$

и последовательно имеем:

$$\begin{gathered}4x\equiv 2 \pmod 7,\\ 4x\equiv 16 \pmod 7,\\ x\equiv 4 \pmod 7,\\ x=7t+4;\end{gathered}$$

далее по указанной формуле имеем:

$$y=\frac{58-11\cdot 4}{7}-11t,$$

откуда

$$y=2-11t.$$

Достаточно положить $t=0$. Получим

$$x=4,\ y=2$$

и окончательно

$$\frac{58}{77}=\frac{4}{7}+\frac{2}{11}.$$

Упражнения

1. Нижеследующие рациональные числа разложить в непрерывные дроби:

а) $\frac{83}{19}$; б) $\frac{121}{27}$; в) $\frac{163}{59}$; г) $\frac{19}{37}$; д) $\frac{23}{47}$; е) $\frac{41}{59}$;

ж) $\frac{37}{61}$; з) $-1\frac{17}{57}$; и) $-\frac{37}{81}$; к) $-\frac{19}{47}$; л) $-\frac{83}{17}$.

2. Даны непрерывные дроби:

а) $[2, 1, 3, 4, 1, 2]$, г) $[0, 1, 2, 4, 5]$, ж) $[2, 1, 3, 4, 1, 2]$,
б) $[0, 3, 1, 2, 7]$, д) $[-2, 1, 2, 2, 1, 5]$ з) $[3, 1, 4, 2, 5]$,
в) $[3, 1, 1, 6, 8]$, е) $[-1, 1, 1, 2, 9]$, и) $[4, 1, 3, 2, 5]$.

Найти соответственно равные им рациональные числа.

3. Решить сравнения:

а) $97x \equiv 11 \pmod{41}$,
б) $41x \equiv 7 \pmod{101}$,
в) $81x \equiv 14 \pmod{202}$,
г) $23x \equiv 5 \pmod{71}$,
д) $92x \equiv 20 \pmod{284}$,
е) $11x \equiv 1 \pmod{567}$,
ж) $243x \equiv 271 \pmod{317}$,
з) $37x \equiv 25 \pmod{107}$,
и) $486x \equiv 542 \pmod{634}$,
к) $111x \equiv 75 \pmod{321}$,
л) $101x \equiv 17 \pmod{113}$,
м) $505x \equiv 85 \pmod{565}$,
н) $7x \equiv 5 \pmod{72}$.

4. Используя метод сравнения, решить нижеследующие уравнения

а) $37x+11y=1$, д) $2977x+1469y=13$,
б) $673x+103y=1$, е) $1414x+406y=42$,
в) $52x+23y=1$, ж) $4997x+4009y=3$
г) $253x+1001y=22$,

в целых числах.

5. Разложить дробь $\frac{13}{15}$ на сумму или разность двух дробей соответственно со знаменателями 3 и 5.

6. Разложить дробь $\frac{19}{21}$ на сумму или разность двух дробей соответственно со знаменателями 3 и 7.

7. Разложить дробь $\frac{37}{55}$ на сумму или разность двух дробей соответственно со знаменателями 5 и 11.

8. Разложить дробь $\frac{12}{35}$ на сумму или разность двух дробей соответственно со знаменателями 5 и 7.

9. Разложить дробь $\frac{68}{143}$ на сумму или разность двух дробей соответственно со знаменателями 11 и 13.

§ 6. ЧИСЛОВЫЕ ФУНКЦИИ. ПРОСТЫЕ ЧИСЛА.

Ш. Х. Михелович. Теория чисел, стр. 49—50, 52—56, 229—232.

А. А. Бухштаб. Теория чисел, стр. 48—51, 92—95, 315—319, 355—358.

Л. Я. Окунев. Краткий курс теории чисел. М., Учпедгиз, 1956, стр. 89—91.

Вопросы для самопроверки

1. Дайте определение функции, выражающей целую часть действительного числа α, т. е. $[\alpha]$.
2. Дайте определение функции $B(x; p_1, p_2, ..., p_k)$.
3. Сформулируйте основные свойства числовой функции Эйлера.
4. Дайте определение совершенных чисел и напишите соответствующую формулу.
5. Дайте определение дружественных чисел и напишите соответствующую формулу.
6. Напишите формулы для вычисления $S(n)$ и $\tau(n)$.
7. Дайте определение чисел «близнецов». Приведите примеры.
8. Сформулируйте проблему Гольдбаха—Эйлера.

Разберите решения примеров, рассмотренных ниже.

Пример 1. Найти число натуральных чисел в интервале от 1 до 103, делящихся на 7.

Решение. Известно, что среди всех натуральных чисел от 1 до m чисел, делящихся на b, будет $\left[\frac{m}{b}\right]$.

Следовательно, в данном случае мы должны вычислить значение функции $\left[\frac{103}{7}\right]$, т. е. найти целую часть числа $\frac{103}{7}$.

Ответ. 14.

Пример 2. Найти число натуральных чисел от 120 до 315, делящихся на 11.

Решение. В соответствии с указаниями к решению примера 1 найдем число натуральных чисел от 1 до 315, делящихся на 11, получим $\left[\frac{315}{11}\right] = 28$, аналогично для чисел, от 1 до 119 имеем: $\left[\frac{119}{11}\right] = 10$, и, следовательно,

число натуральных чисел от 120 до 315, делящихся на 11, будет равно

$$28-10=18.$$

Пример 3. Найти количество целых положительных чисел, не превосходящих числа 107 и не делящихся ни на одно из простых чисел 3, 5 и 7.

Решение. Возьмем числовую функцию $B(x;\ p_1,\ p_2,\ \ldots,\ p_k)$ и применим к рассматриваемому упражнению. Получим:

$$B(107;\ 3,\ 5,\ 7)=[107]-\left[\frac{107}{3}\right]-\left[\frac{107}{5}\right]-\left[\frac{107}{7}\right]+$$
$$+\left[\frac{107}{3\cdot5}\right]+\left[\frac{107}{3\cdot7}\right]+\left[\frac{107}{5\cdot7}\right]-\left[\frac{107}{3\cdot5\cdot7}\right]=$$
$$=107-35-21-15+7+5+3-1=50.$$

Пример 4. Используя свойства функции $[x]$, разложить на простые множители число 30!.

Решение. Искомое разложение, очевидно, имеет следующий вид:

$$30!=2^{\alpha_1}\cdot3^{\alpha_2}\cdot5^{\alpha_3}\cdot7^{\alpha_4}\cdot11^{\alpha_5}\cdot13^{\alpha_6}\cdot17^{\alpha_7}\cdot19^{\alpha_8}\cdot23^{\alpha_9}\cdot29^{\alpha_{10}}.$$

Итак, решение задачи сводится к нахождению показателей, с которыми входят простые числа от 2 до 30 в разложение 30!.

В число 30! множитель 2 входит с показателем

$$\alpha_1=\left[\frac{30}{2}\right]+\left[\frac{30}{4}\right]+\left[\frac{30}{8}\right]+\left[\frac{30}{16}\right]=26.$$

Множитель 3 входит с показателем

$$\alpha_2=\left[\frac{30}{3}\right]+\left[\frac{30}{9}\right]+\left[\frac{30}{27}\right]=14.$$

Множитель 5— с показателем

$$\alpha_3=\left[\frac{30}{5}\right]+\left[\frac{30}{25}\right]=7.$$

Таким же образом легко показать, что множители 7, 11, 13, 17, 19, 23 и 29 входят соответственно с показателями 4, 2, 2, 1, 1, 1, 1.

Итак, искомое разложение имеет вид:

$$30!=2^{26}\cdot3^{14}\cdot5^7\cdot7^4\cdot11^2\cdot13^2\cdot17\cdot19\cdot23\cdot29.$$

Пример 5. Найти показатель, с которым число 3 содержится в числе

$$\frac{50!}{25! \cdot 25!}.$$

Решение. Найдем, с каким показателем входит 3 в произведение 50!:

$$\left[\frac{50}{3}\right] + \left[\frac{50}{9}\right] + \left[\frac{50}{27}\right] = 22;$$

аналогично находим, с каким показателем входит 3 в произведение 25!:

$$\left[\frac{25}{3}\right] + \left[\frac{25}{9}\right] = 10.$$

Следовательно, показатель, с которым число 3 содержится в числе $\frac{50!}{25! \cdot 25!}$, равен $22-2 \cdot 10=2$.

Пример 6. Показать, что $\frac{30!}{15! \cdot 15!}$ делится на произведение $17 \cdot 19 \cdot 23 \cdot 29$.

Решение. Воспользуемся свойством: $\frac{(2n)!}{n!\,n!}$ делится на произведение Π_p, где p — простое число; $n<p \leqslant 2n$.

В предложенном примере $n=15$,

$$\Pi_p = 17 \cdot 19 \cdot 23 \cdot 29.$$

Следовательно, $\frac{30!}{15! \cdot 15!} \vdots 17 \cdot 19 \cdot 23 \cdot 29$.

Если не пользоваться свойством в окончательном виде, то предложенное упражнение может быть решено следующим образом: $\frac{30!}{15! \cdot 15!}$ можно рассматривать как коэффициент C_{30}^{15} при x^{15} в разложении

$$(1+x)^{30},$$

и, следовательно, $\frac{30!}{15! \cdot 15!}$ — целое положительное число. Так как

$$30! \vdots 17 \cdot 19 \cdot 23 \cdot 29,$$

а $(15!,\ 17 \cdot 19 \cdot 23 \cdot 29) = 1$, то частное от деления $\frac{30!}{15! \cdot 15!}$ на $17 \cdot 19 \cdot 23 \cdot 29$ является целым числом.

Пример 7. Найти число натуральных чисел, не превышающих 450 и имеющих с 450 наибольшим общим делителем число 15.

Решение. Используем свойство функции Эйлера: если d — делитель числа n, то число натуральных чисел, не превышающих n и имеющих с n общим наибольшим делителем число d, равно $\varphi\left(\frac{n}{d}\right)$.

Так как $\frac{n}{d}=\frac{450}{15}=30$, то $\varphi\left(\frac{n}{d}\right)=\varphi(30)$, где $\varphi(30)$ — число натуральных чисел, не превышающих числа 30 и взаимно простых с 30. Для вычисления $\varphi(30)$ воспользуемся формулой для вычисления функции Эйлера:

$$\varphi(n)=p_1^{\alpha_1-1}\cdot p_2^{\alpha_2-1}\cdot\ldots\cdot p_k^{\alpha_k-1}(p_1-1)(p_2-1)\ldots(p_k-1),$$

где $p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ — каноническое разложение числа n.

Так как $30=2\cdot3\cdot5$, то $\varphi(30)=(3-1)(5-1)=8$.

Пример 8. Проверить для числа $n=8$ справедливость формулы $\sum\limits_{d/n}\varphi(d)=n$, где суммирование распространено на все положительные делители числа n.

Решение. Выпишем все положительные делители числа 8, а именно:

$$1,\ 2,\ 4,\ 8.$$

Применяя соответствующие формулы, находим, что $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(4)=2$, $\varphi(8)=4$, следовательно, $\varphi(1)+\varphi(2)+\varphi(4)+\varphi(8)=1+1+2+4=8$, т. е. данному числу.

Пример 9. Найти сумму и число делителей числа 600.

Решение. Если каноническое разложение данного числа имеет вид

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k},$$

то сумма делителей вычисляется по формуле:

$$S(a)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1},$$

а число делителей $\tau(a)$ по формуле

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

Для данного примера имеем:

$$600=2^3\cdot3\cdot5^2.$$

$$S(600)=\frac{2^4-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^3-1}{5-1}=1860,$$

$$\tau(600)=(3+1)(1+1)(2+1)=24.$$

Пример 10. Найти сумму делителей числа 496, отличных от несобственного делителя данного числа.

Решение. Поступая, как при решении предыдущего примера, имеем:

$$496=2^4\cdot31,$$

$$S(496)=\frac{2^5-1}{2-1}\cdot\frac{31^2-1}{31-1}=992.$$

Несобственный делитель данного числа равен самому числу, т. е. 496, откуда

$$S(496)-496=992-496=496.$$

Число, удовлетворяющее требованию $S(a)-a=a$, называется совершенным. Таким образом, число 496 — совершенное число.

Пример 11. Найти сумму делителей чисел 220 и 284, отличных от несобственных делителей данных чисел.

Решение. а) $220=2^2\cdot5\cdot11$,

$$S(220)=\frac{2^3-1}{2-1}\cdot\frac{5^2-1}{5-1}\cdot\frac{11^2-1}{11-1}=504,$$

$$S(220)-220=504-220=284;$$

б) $284=2^2\cdot71$,

$$S(284)-284=504-284=220.$$

Если для двух чисел a и b выполняются условия $S(a)-a=b$, $S(b)-b=a$, то такие числа называются дружественными.

Следовательно, 220 и 284 — дружественные числа.

Пример 12. Найти все делители числа 90.

Решение. Возьмем каноническое разложение некоторого числа

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}.$$

Тогда для суммы делителей этого числа получим формулу:

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

Воспользуемся этой формулой для решения предложенного примера:

$$90=2\cdot3^2\cdot5;$$
$$S(90)=(1+2)(1+3+3^2)(1+5);$$

перемножая почленно, получим все делители данного числа: 1, 2, 3, 6, 9, 18, 5, 10, 15, 30, 45, 90. Легко проверить, все ли делители найдены, воспользовавшись формулой

$$\tau(90)=2\cdot3\cdot2=12.$$

Пример 13. Если обозначить через $S_k(m)$ сумму k-степеней всех делителей числа

$$m=p^{\alpha}\cdot q^{\beta}\cdot\ldots\cdot r^{\gamma},$$

то справедлива формула:

$$S_k(m)=\frac{p^{(\alpha+1)k}-1}{p^k-1}\cdot\frac{q^{(\beta+1)k}-1}{q^k-1}\cdot\ldots\cdot\frac{r^{(\gamma+1)k}-1}{r^k-1}$$

(см. А. К. Сушкевич. Теория чисел. Харьков, 1954, стр. 25, упражнение 15). На основании этой формулы вычислить $S_2(24)$.

Решение. Так как

$$24=2^3\cdot3,$$
$$S_2(24)=\frac{2^{4\cdot2-1}}{2^2-1}\cdot\frac{3^{2\cdot2}-1}{3^2-1}=85\cdot10=850.$$

Пример 14. Найти $\pi(30)$.

Решение. На основании определения, числовая функция $\pi(x)$ означает количество простых чисел, не превосходящих действительного числа $x>1$.

Воспользуемся приемом, известным под названием решета Эратосфена. Выпишем все натуральные числа от 2 до 30, а именно: 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, и, вычеркивая все составные числа (процесс известен из курса элементарной математики), сохраняем в этой по-

следовательности только простые числа: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Подсчитав количество чисел в этой последовательности, получим

$$\pi(30)=10.$$

Для решения этого примера можно воспользоваться формулой:

$$\pi(x)=B(x;\ p_1,\ p_2,\ \ldots,\ p_k)+k-1,$$

где $p_1,\ p_2,\ \ldots,\ p_k$ — последовательность простых чисел 2, 3, ..., и $p_k \geqslant \sqrt{x}$ (см. Л. Я. Окунев. Краткий курс теории чисел, стр. 122, задача 13). Известно, что если число, не превышающее числа x, есть составное, то наименьший его простой делитель $p \leqslant \sqrt{x}$; значит, функция $B(x_1;\ p_1,\ p_2,\ \ldots,\ p_k)$ дает количество простых чисел последовательности натуральных чисел от $[\sqrt{x}+1]$ до $[x]$, увеличенное на 1, т. е. включено число единица; присоединяя число k, уменьшенное на 1, получим указанную формулу.

Применяя формулу к рассматриваемому примеру, получим:

$$\pi(30)=[30]-\left[\frac{30}{2}\right]-\left[\frac{30}{3}\right]-\left[\frac{30}{5}\right]+\left[\frac{30}{2\cdot 3}\right]+\left[\frac{30}{2\cdot 5}\right]+$$
$$+\left[\frac{30}{3\cdot 5}\right]-\left[\frac{30}{2\cdot 3\cdot 5}\right]+3-1=10.$$

Пример 15. Показать, что существует бесконечное множество простых чисел вида $3n-1$.

Решение. Все множество натуральных чисел разобьем на три подмножества с общими членами: $3u,\ 3u+1,\ 3u+2$ (или $3n-1$); среди чисел первого подмножества имеется лишь одно простое число 3, остальные простые числа входят в последние два подмножества. Допустим, что P — наибольшее простое число вида $3n-1$; напишем число

$$N=3\cdot 2\cdot 5\cdot 8\cdot 11\cdot 17\cdot \ldots \cdot P-1,$$

где в произведение включено число 3 и все простые числа вида $3n-1$; очевидно, число N будет вида $3n-1$ и, следовательно, $N=3s-1$.

Число N не может быть простым, так как $N>P$, но оно не может иметь простыми делителями число 3 и чис-

ла вида $3n-1$; следовательно, все его простые делители вида $3u+1$, откуда $N=3t+1$, но равенство

$$3t+1=3s-1$$

невозможно ни при каких целых положительных значениях t и s, так как последнее равенство может быть переписано в виде

$$3(s-t)=2,$$

где левая часть кратна трем, а 2 не $\vdots$ 3. Полученное противоречие доказывает существование бесконечного множества простых чисел вида $3n-1$.

Пример 16. Показать, что из справедливости теоремы о представлении всякого нечетного числа, большего 5, в виде суммы трех простых чисел, доказанной академиком И. М. Виноградовым, вытекает справедливость теоремы о представлении четного числа, начиная с 10, в виде суммы четырех простых чисел.

Решение. На основании данной теоремы имеем:

$$2n-1=p_1+p_2+p_3,$$

откуда

$$2n+2=3+p_1+p_2+p_3.$$

Пример 17. Показать, что тройки чисел вида

$$p,\ p+2,\ p+4$$

не могут быть простыми.

Решение. Если $p=2$, то $p+2=4$ — составное число; напишем формулу нечетного числа $p=2k+1$, тогда $p+2=2k+3$, $p+4=2k+5$, где k пробегает все множество натуральных чисел. Это множество может быть разбито на три подмножества с общими членами: $k=3u$, $k=3u+1$, $k=3u+2$; если $k=3u$, то $p+2=6u+3$ и $p+2\vdots 3$; если $k=3u+1$, то $p=6u+3$ и $p\vdots 3$, наконец, если $k=3u+2$, то $p+4=6u+9$ и $(p+4)\vdots 3$.

Замечание. Установлено существование троек простых чисел вида p, $p+2$, $p+6$ и четверок простых чисел вида p, $p+2$, $p+6$, $p+8$.

Упражнения

1. Найти количество натуральных чисел:
а) в интервале от 1 до 177, делящихся на 5,
б) в интервале от 1 до 239, делящихся на 11,
в) в интервале от 1 до 241, делящихся на 13,

г) в интервале от 1 до 307, делящихся на 17,

д) в интервале от 1 до 347, делящихся на 19.

2. Найти количество натуральных чисел:

а) в интервале от 141 до 257, делящихся на 5,

б) в интервале от 80 до 280, делящихся на 7,

в) в интервале от 100 до 367, делящихся на 11,

г) в интервале от 200 до 507, делящихся на 13,

д) в интервале от 220 до 577, делящихся на 19.

3. Найти количество натуральных чисел:

а) не превосходящих числа 1317 и не делящихся ни на одно из простых чисел 2, 3, 5;

б) не превосходящих числа 1420 и не делящихся ни на одно из простых чисел 2, 7, 11;

в) не превосходящих числа 721 и не делящихся ни на одно из простых чисел 3, 11, 13;

г) не превосходящих числа 423 и не делящихся ни на одно из простых чисел 2, 3, 5, 7;

д) не превосходящих числа 347 и не делящихся ни на одно из простых чисел 2, 3, 7, 11;

е) не превосходящих числа 1215 и не делящихся ни на одно из простых чисел 3, 5, 7, 13.

4. Найти показатель, с которым:

а) число 3 входит в произведение 28!,

б) число 7 входит в произведение 52!,

в) число 5 входит в произведение 50!,

г) число 2 входит в произведение 33!,

д) число 11 входит в произведение 120!.

5. Используя свойства функции $[x]$, разложить на простые множители числа: а) 13!, б) 15!, в) 17!, г) 18!, д) 20!, е) 24!, ж) 27!.

6. Найти показатель, с которым:

а) число 2 сдержится в числе $\frac{20!}{10!\cdot 10!}$,

б) число 3 содержится в числе $\frac{40!}{20!\cdot 20!}$,

в) число 5 содержится в числе $\frac{50!}{25!\cdot 25!}$,

г) число 7 содержится в числе $\frac{60!}{30!\cdot 30!}$,

д) число 11 содержится в числе $\frac{90!}{45!\cdot 45!}$.

7. Найти количество натуральных чисел, не превышающих числа 1000 и имеющих с ним наибольшим общим делителем число 20.

8. Найти количество натуральных чисел, не превышающих числа 1200 и имеющих с ним наибольшим общим делителем число 30.

9. Найти количество натуральных чисел, не превышающих числа 1800 и имеющих с ним наибольшим общим делителем число 36.

10. Найти количество натуральных чисел, не превышающих числа 2400 и имеющих с ним наибольшим общим делителем число 40.

11. Найти количество натуральных чисел, не превышающих числа 2600 и имеющих с ним наибольшим общим делителем число 52.

12. Проверить справедливость формулы

$$\sum_{d/n} \varphi(d) = n,$$

где суммирование распространено на все положительные делители числа n, для чисел:

а) 16, б) 20, в) 21, г) 30, д) 40.

13. Найти сумму и количество делителей чисел:

а) 300, б) 420, в) 480, г) 560, д) 230, е) 290, ж) 620.

14. Найти сумму, количество делителей и все делители чисел:

а) 12, б) 16, в) 20, г) 40, д) 60.

15. Вычислить: а) $\pi(40)$, б) $\pi(60)$, в) $\pi(90)$.

16. Доказать, что существует бесконечное множество простых чисел вида $3n+1$.

17. Доказать, что существует бесконечное множество простых чисел вида $4n+1$.

18. Доказать, что существует бесконечное множество простых чисел вида $6n-1$.

19. Доказать, что существует бесконечное множество простых чисел вида $4n-1$.

20. Доказать, что существует бесконечное множество простых чисел вида $6n+1$.

ЧАСТЬ II

ДОПОЛНИТЕЛЬНЫЕ ЗАДАЧИ ДЛЯ САМОСТОЯТЕЛЬНОГО РЕШЕНИЯ

§ 1. КЛАССЫ ПО ДАННОМУ МОДУЛЮ. СРАВНЕНИЯ И КЛАССЫ

1. Доказать, что если $n \geqslant 3$, то $\varphi(n)$ — четное число.

2. Известно, что $\varphi(n) = 252$, каноническое разложение числа n имеет вид $n = p_1^{\alpha_1} p_2^{\alpha_2}$, где $\alpha_1 > 1$ и $\alpha_2 > 1$; найти число n. Ответ: 441.

3. Каноническое разложение числа n содержит лишь простые числа 3, 5 и 11, $\varphi(n) = 3600$; найти число n. Ответ: 7425.

4. Доказать, что если m и n — любые целые положительные числа, то по крайней мере одно из них, либо их сумма, либо их разность, делится на число 3.

5. Доказать, что если числа a и n взаимно просты, $ad-bc$ и $a-b$ делятся на n, то $d-c$ делится на n.

6. Доказать, что a^m-b^m, где $a > b$, m — целое положительное число, делится на разность $a-b$.

Указание. Предварительно доказать, что числа a и b, где $a > b$, при делении на их разность $a-b$ дают одинаковые остатки.

7. Доказать, что квадрат простого числа p, уменьшенный на единицу, где p отлично от чисел 2 и 3, делится на на 12.

8. Доказать, что если p — простое число, то

$$C_{p-1}^{k} \equiv (-1)^k \pmod{p}.$$

Указание. Использовать сравнения вида

$$p-k+i \equiv -(k-i) \pmod{p}.$$

9. Доказать, что если число 2^m-1, где m — целое положительное число, есть число простое, то и m — простое число.

10. Доказать, что если p — простое число, то

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Указание. Воспользоваться формулой бинома Ньютона.

11. Доказать, что если $(a, m)=1$, то числа

$$a, 2a, \ldots, (m-1)a, ma$$

образуют полную систему вычетов по модулю m.

12. Доказать, что сумма чисел, составляющих приведенную систему наименьших положительных вычетов по модулю m, кратна m.

13. Показать, что $(73^{12}-1)$ делится на число 105.

14. Доказать, что если p — простое число, то произведение $2\cdot 3\cdot \ldots \cdot (p-3)\,(p-2)$ при делении на число p дает в остатке единицу.

15. Найти остаток от деления числа 3^{301} на число 1000.

Указание. Представить $1000=8\cdot 125$ и применить теорему Эйлера о сравнении. Ответ: 3.

16. Показать, что если $(a, 42)=1$, то $a^{18}\equiv 1 \pmod{42}$.

Указание. Представить $42=7\cdot 3\cdot 2$, рассматривая эти числа, как модули.

§ 2. СРАВНЕНИЯ С НЕИЗВЕСТНОЙ ВЕЛИЧИНОЙ

1. Показать, что сравнение $(m-1)!+1\equiv 0 \pmod{m}$, где m — составное число, не имеет места.

2. Доказать, что если p — простое число, то

$$(p-2)!\equiv 1 \pmod{p}.$$

3. Доказать, что если p — простое число, $p\equiv 1 \pmod 4$, то сравнение $x^2\equiv -1 \pmod{p}$ имеет решение.

Указание. Воспользоваться теоремой Вильсона и сравнениями вида $p-k\equiv -k \pmod{p}$.

4. Доказать, что если функция $f(x)$ неприводима по модулю p и степень ее выше первой, то сравнение $f(x)\equiv 0 \pmod{p}$ не имеет решений.

5. Показать, что если модуль есть нечетное число, то сравнение

$$ax^2+bx+c\equiv 0 \pmod{2k+1}$$

можно свести к сравнению

$$z^2\equiv l \pmod{2ka+a}.$$

6. Исследовать и решить сравнение $x^2\equiv a \pmod 4$, если a — нечетное число. Ответ: $x\equiv 1;\ 3 \pmod 4$.

7. Исследовать и решить сравнение $x^2\equiv a \pmod 8$, если a — четное число.

8. Показать, что решением сравнения $x^2 \equiv a \pmod{p}$, где $p=4m+3$, $(a, p)=1$, является $x=\pm a^{m+1} \pmod{p}$.

Указание. Следует рассмотреть сравнение $a \equiv x^2 \pmod{p}$, а затем возвести обе части сравнения в степень $\frac{p-1}{2}=2m+1$.

9. Показать, что решением сравнения $x^2 \equiv a \pmod{p}$, где $p=8m+5$, $(a, p)=1$, является либо $x=\pm a^{m+1} \pmod{p}$, либо $x=\pm 2^{2m+1} \pmod{p}$.

10. Показать, что сравнение $x^2 \equiv 1 \pmod{p^k}$, где p — простое нечетное число, k — натуральное число, имеет два различных решения.

11. Показать, что среди всех чисел, составляющих полную систему наименьших неотрицательных вычетов по модулю m, сравнимы с полными квадратами не более чем $\frac{m}{2}+1$ чисел, если m — четное число, и не более $\frac{m+1}{2}$ чисел, если m — нечетное число.

12. Доказать, что сумма наименьших положительных квадратичных невычетов по простому модулю $p>3$ кратна p.

13. Доказать, что произведение чисел

$$a, b, \ldots, c$$

дает квадратичный вычет или невычет по простому модулю p в зависимости от четности или нечетности количества вычетов среди сомножителей.

Указание. Воспользоваться равенством:

$$(a \cdot b \cdot \ldots \cdot c)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \cdot \ldots \cdot c^{\frac{p-1}{2}}.$$

14. Для каждого простого числа $p \equiv 1 \pmod{4}$ сравнение $x^2 \equiv -1 \pmod{p}$ имеет решение; показать справедливость этого положения.

15. Доказать невозможность равенства

$$\left(\frac{q}{p}\right) = -\left(\frac{q_1}{p}\right),$$

где $\left(\frac{q}{p}\right)$ — знак символа Лежандра, $q \equiv q_1 \pmod{p}$, где p — простое число, большее 2.

16. Доказать, что

$$\left(\frac{q^n}{p}\right) = \left(\frac{q}{p}\right)^n,$$

где $\left(\frac{q}{p}\right)$ — знак символа Лежандра.

17. Доказать, что если $x^2+ay^2\equiv 0 \pmod p$, $(x, ay)=1$, то число $-a$ является квадратичным вычетом по модулю p.

18. Показать, что

$$\left(-\frac{2}{p}\right)=\begin{cases} +1, \text{ если } p\equiv 1 \pmod 8,\ p\equiv 7 \pmod 8, \\ -1, \text{ если } p\equiv 3 \pmod 8,\ p\equiv 5 \pmod 8. \end{cases}$$

§ 3. СТЕПЕННЫЕ ВЫЧЕТЫ

1. Доказать, что если число a принадлежит показателю δ по простому модулю p и $(k, \delta)=\alpha$, то число a^k принадлежит показателю $\frac{\delta}{\alpha}$ по модулю p.

2. Зная, что числа 12 и 23 принадлежат соответственно показателям 4 и 7 по модулю 29, найти, какому показателю принадлежит число 15 по модулю 29. Ответ: Показателю 28.

3. Число a принадлежит показателю δ по простому модулю p, где $\delta<p-1$. Даны последовательности:

$$1, a, a^2, \ldots, a^{\delta-1}, \tag{1}$$

$$b, ba, ba^2, \ldots, ba^{\delta-1}, \tag{2}$$

где $(b, p)=1$ и число b несравнимо по модулю p ни с одним из чисел последовательности (1). Показать, что числа последовательностей являются представителями различных классов по модулю p и взаимно просты с p.

4. Показать, что если $(a, p)=1$, где p — простое число, $a^{2k}\equiv 1 \pmod p$ и число a принадлежит показателю $2k$ по модулю p, то $a^k\equiv -1 \pmod p$.

Указание. Исследовать сравнение $(a^k-1)(a^k+1)\equiv 0 \pmod p$.

5. Доказать, что если

$a^{\alpha_1}\equiv 1 \pmod{m_1}$, $a^{\alpha_2}\equiv 1 \pmod{m_2}$,..., $a^{\alpha k}\equiv 1 \pmod{m_k}$, то $a^{\beta}\equiv 1 \pmod m$, где β—наименьшее общее кратное чисел $\alpha_1, \alpha_2, \ldots, \alpha_k$, а число m — наименьшее общее кратное чисел $m_1, m_2 \ldots, m_k$.

6. Доказать, что если число a — первообразный корень простого модуля p, то a^k, где $(k, p-1)=1$, также является первообразным корнем по модулю p.

7. Показать, что если p — простое число вида $4k+1$ и число a — первообразный корень по модулю p, то число $p-a$ также первообразный корень по модулю p.

8. Зная, что число 2 — первообразный корень по модулю 37, показать, что имеет место сравнение $2^{18} \equiv 36 \pmod{37}$.

9. Показать, что по модулю 36 не существует первообразных корней.

10. Доказать, что если числа a и b являются первообразными корнями по простому модулю $p > 2$, то произведение $a \cdot b$ не может быть первообразным корнем по модулю p.

11. Зная, что число 2 — первообразный корень по модулю 131, решить сравнение $x^3 \equiv 16 \pmod{131}$. Ответ: $x \equiv 108 \pmod{131}$.

12. Показать, что

$$\operatorname{ind} 1 + \operatorname{ind} 2 + \ldots + \operatorname{ind}(p-2) \equiv 0 \pmod{p-1}.$$

13. Зная, что $\operatorname{ind}_3 19 \equiv 4 \pmod{30}$, $\operatorname{ind}_{17} 3 \equiv 13 \pmod{30}$, где числа 3 и 17 являются первообразными корнями по модулю 31, найти $\operatorname{ind}_{17} 19$. Ответ: $\operatorname{ind}_{17} 19 \equiv 22 \pmod{30}$.

14. Взяв таблицу индексов при основании, равном 2, для модуля 13 и зная, что $\operatorname{ind}_6 2 \equiv 5 \pmod{12}$, составить таблицу индексов, приняв за основание первообразный корень 6.

15. Доказать, что первообразные корни по модулю p^α (если они существуют) являются одновременно первообразными корнями по модулю p, где p — простое число.

Указание. Использовать равенство $a^\delta = 1 + pN$, где N — целое число и δ — показатель, которому принадлежит число a по модулю p.

16. С помощью таблиц индексов найти классы вычетов четвертой степени по модулю 13. Ответ: $\overline{1}, \overline{3}, \overline{9}$.

17. Установить, является число 3 вычетом или невычетом пятой степени по модулю 29.

Указание. Исходить из сравнения $x^n \equiv a \pmod{p}$, где $(a, p) = 1$; если $(n, p-1) = \delta$ и $a^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$, то число a вычет степени n по модулю p. Ответ: вычет.

18. Пользуясь теорией индексов, вывести критерий Эйлера для квадратичных вычетов.

Указание. В качестве исходного сравнения взять сравнение $x^2 \equiv a \pmod{p}$, где $(a, p) = 1$, и проиндексировать это сравнение.

19. Основываясь на теореме: «Если g — первообразный корень по простому модулю p, то g^{2k} и g^{2k+1} соот-

ветственно являются квадратичным вычетом и квадратичным невычетом по модулю p», показать, что существует $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ невычетов по модулю p.

Указание. Если g — первообразный корень по модулю p, то в качестве приведенной системы вычетов по модулю p, взять числа

$$g^1, g^2, g^3, \ldots, g^{p-1}.$$

§ 4. АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

1. Показать, что разность $(a+1)(a+2)\ldots(a+n)-n!$ всегда делится на a.

2. Показать, что если $(a, 12)=(b, 12)=1$, то число $a^{96}-b^{96}$ делится на 144.

3. Показать, что если $(a, 8)=(b, 8)=1$, то число $a^9-ab^8+a^8b-b^9$ делится на 8.

4. Показать, что если $(a, 7)=(b, 7)=1$, то число $a^8b^6-a^6b^8-a^2+b^2$ делится на 7.

5. Доказать, что сумма данного числа и числа, написанного теми же цифрами, но взятыми в обратном порядке, делится на число 11, если количество цифр данного числа четное.

6. Доказать, что если к любому трехзначному числу приписать справа такое же число, то полученное число будет делиться на числа 7, 11 и 13.

7. Написать пятизначные числа, средние цифры которых составляют число 809, делящиеся на 55. Ответ: 18095 и 68090.

8. Показать, что если число $\overline{a_2a_1a_0}$ делится на 27 или 37, то число $\overline{a_1a_0a_2}$ делится на 27 или 37.

Указание. Воспользоваться сравнением $100a_2+10a_1+a_0\equiv 0 \pmod{27}$ и свойствами сравнений.

9. Доказать, что если $(a, b)=1$ и из двух чисел $11a+2b$ и $18a+5b$ одно кратно числу 19, то $(11a+2b, 18a+5b)=19$.

10. Найти число $\overline{4415xy}$, делящееся на 999. Ответ: 441558.

11. Найти число $\overline{2485xyz}$, делящееся на 1001. Ответ: 2485483.

12. Найти число вида $\overline{1xy71}$, делящееся на 33.

13. Найти число $\overline{xy3242}$, делящееся на 198.

14. Возьмите многозначное число, в любом порядке переставьте его цифры и из большего отнимите меньшее; в полученной разности зачеркните одну цифру и подсчитайте сумму сохранившихся цифр. Как, зная последнюю, установить, какая цифра зачеркнута? Дайте теоретическое обоснование методу.

§ 5. НЕПРЕРЫВНЫЕ ДРОБИ

1. Доказать, что при $n \geqslant 2$ справедливо

$$Q_{n-2}P_n - P_{n-2}Q_n = (-1)^n g_n.$$

2. На основании свойств подходящих дробей доказать, что уравнение $ax+by=1$, где $(a, b)=1$, всегда имеет решение в целых числах.

Указание. Воспользоваться равенством $\frac{P_n}{Q_n} = \frac{a}{b}$ и свойством

$$Q_{n-1}P_n - P_{n-1}Q_n = (-1)^{n-1}.$$

3. На основании существования решения в целых числах уравнения $ax+by=1$, где $(a, b)=1$, доказать, что если $(a, b)=1$, $c \vdots a$, $c \vdots b$, то $c \vdots ab$.

4. На основании существования решения в целых числах уравнения $ax+by=1$, где $(a, b)=1$, доказать, что если $(a, c)=1$, $(b, c)=1$, то $(ab, c)=1$.

5. Сумма произведений двух целых чисел соответственно на 7 и на 3 равна 41; найти эти числа.

6. На основании существования решения в целых числах уравнения $ax-by=1$, где $(a, b)=1$, показать, что в окружность посредством циркуля и линейки можно вписать правильный двенадцатиугольник.

§ 6. ЧИСЛОВЫЕ ФУНКЦИИ. ПРОСТЫЕ ЧИСЛА

1. Среди чисел от 1 до n найти количество чисел, которые делятся на p^k, но не делятся на p^{k+1}, где p — простое число и $p<n$. Ответ: $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$.

2. Среди чисел от 1 до 41 найти количество чисел, делящихся на 2, но не делящихся на 2^3.

Указание. Применить функцию $[x]$. Ответ: 15.

3. Найти показатель, с которым число 12 входит в произведение 37!.

4. Найти показатель, с которым число 24 входит в произведение 50!. Ответ: 12.

5. Представить произведение всех натуральных чисел от 21 до 40 в виде произведения простых чисел.

6. Найти, при каком целом положительном значении x уравнение $[2,5x]=100$ имеет решение. Ответ: $x=40$.

7. Доказать, что если $n\geqslant 3$, то $\varphi(n)$ — четное число.

8. На основании свойств числовой функции Эйлера доказать, что в последовательности натуральных чисел существует бесконечное множество простых чисел.

Указание. Допустив, что p_k — наибольшее простое число, воспользоваться равенством $n=p_1\cdot p_2\cdot\ldots\cdot p_k$.

9. Дано: а) $\varphi(n)=48$; $n=2^{\alpha}\cdot 3^{3}\cdot 5^{\gamma}\cdot 7^{\xi}$; б) $\varphi(n)=320$; $n=2^{\alpha}\cdot 3^{\beta}\cdot 5^{\gamma}$. Найти n. Ответ: а) 210, б) 1200.

10. Проверить справедливость равенства $\varphi(240)=\varphi(160)$.

11. Найти условия, при которых $\varphi(3x)=\varphi(2x)$, где x — натуральное число.

12. Показать невозможность равенства $\varphi(2x)=\varphi(5x)$, где x — натуральное число.

13. Найти $\tau(a^3)$, если $\tau(a)=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_k+1)$.

14. Найти $\tau(a^3)$, если $a=p_1^{\alpha}p_2^{\beta}$, $\tau(a^2)=15$, где p_1 и p_2 — простые числа. Ответ: 28.

15. Найти количество делителей числа n^3, если $n=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$ и число n^2 имеет 105 различных делителей. Ответ: 280.

16. Найти наименьшее натуральное число, имеющее восемь положительных делителей. Ответ: 24.

17. Найти наименьшее натуральное число, имеющее двенадцать положительных делителей. Ответ: 60.

18. Доказать, что существует бесконечное множество простых чисел в последовательности натуральных чисел, исходя из допущения существования наибольшего простого числа p и исследования суммы

$$S=(p_1p_2\ldots p_k)+(q_1q_2\ldots q_s),$$

где в правую часть равенства включены все простые числа от 2 до p.

19. Доказать, что всякое число вида $3k-1$ либо простое, либо содержит нечетное число простых делителей этого вида.

Указание. Учесть, что все множество простых чисел представимо совокупностями арифметических прогрессий с общими членами $3n$, $3n+1$, $3n-1$.

20. Доказать, что каждое натуральное число вида $4k+3$ имеет по крайней мере один простой делитель того же вида.

21. Зная, что существует бесконечное множество простых чисел вида $3n+1$, доказать существование бесконечного множества простых чисел вида $6k+1$.

Указание. Положить $n=2k$ и $n=2k+1$.

Василий Александрович Александров,
Святослав Михайлович Горшенин
ЗАДАЧНИК-ПРАКТИКУМ ПО ТЕОРИИ ЧИСЕЛ
Редактор **Л. М. Котова**
Технический редактор **Л. Я. Медведев**
Корректор **Н. М. Данковцева**

Сдано в набор 3/XI—1971 г. Подписано к печати 12/IV 1972 г. $84\times108^1/_{32}$ Бумага типогр. № 3. Печ. л. 2,5 Услов. л. 4,2. Уч.-изд. л. 3,63 Тираж 30 тыс. экз. (Пл. 1972 г.) А07191
Издательство «Просвещение» Комитета по печати при Совете Министров РСФСР. Москва, 3-й пр. Марьиной рощи, 41.
Типография № 2 Росглавполиграфпрома, г. Рыбинск, ул. Чкалова, 8. Заказ 3429.
Цена 10 коп.