Г. А. КУДРЕВАТОВ

СБОРНИК ЗАДАЧ ПО ТЕОРИИ ЧИСЕЛ

Г. А. КУДРЕВАТОВ

СБОРНИК ЗАДАЧ ПО ТЕОРИИ ЧИСЕЛ

ИЗДАТЕЛЬСТВО
«ПРОСВЕЩЕНИЕ»
Москва · 1970

517—1
К88

Одобрен Министерством просвещения СССР в качестве учебного пособия для студентов пединститутов

Кудреватов Г. А.

К 88 Сборник задач по теории чисел. М., «Просвещение», 1970.

128 с.

В сборнике содержится около 500 задач по теории чисел. К ним в конце даны ответы, указания или полные решения. Каждый параграф начинается с кратких сведений из теории чисел, необходимых для решения задач.

Сборник предназначен для студентов математических специальностей пединститутов.

$\frac{2\text{-}2\text{-}3}{19\text{—}70}$

517,1

ПРЕДИСЛОВИЕ

Сборник предназначен для студентов математических специальностей пединститутов и составлен в соответствии с программой Министерства просвещения РСФСР по курсу теории чисел для физико-математических факультетов педагогических институтов. В него включена глава «Делимость целых чисел».

Основное внимание уделено задачам, решение которых помогает лучше усваивать понятия и идеи курса, часто имеющие прямое отношение к школьной математике. В сборник включены и задачи несколько повышенной трудности, решение которых может способствовать повышению общей математической культуры и развитию творческих способностей будущего учителя математики. Многие задачи могут быть использованы при работе с учащимися в математическом кружке.

Каждый параграф начинается с кратких сведений из теории, необходимых для решения приводящихся ниже задач.

В ряде случаев для полного уяснения алгоритма решения под одним номером дается несколько однотипных задач (вариантов). В тех же случаях, когда самостоятельное составление однотипных задач не представляет никаких затруднений, в сборнике дается лишь один из вариантов задачи.

Отдельные задачи являются новыми (в использованной литературе не встречаются). К ним относятся, например, задачи 86—88, 115, 122, 128, 129, 144, 190, 199 (5—7), 200 (4—7), 207, 256—274, 330, 412, 432, 434, 442, 458, 466.

Приведены примеры задач, до сих пор не имеющих своего решения. Из задач такого рода выбраны наиболее близко стоящие к кругу вопросов, затронутых в сборнике. Ответы, как и условия соответствующих задач, даны в одних и тех же системах счисления.

В связи с тем что решение задач по теории чисел нередко вызывает затруднения (особенно у студентов-заочников), в конце сборника даны не только ответы, но и указания и даже решения (в ряде случаев решения отличны от встречающихся в литературе).

В целях удобства пользования сборником он снабжен таблицей простых чисел и таблицами индексов.

При составлении сборника автор старался максимально использовать уже накопленный в этой области опыт (использованная литература приводится).

Автор не считает настоящий сборник свободным от недостатков и будет благодарен за все замечания, направленные на его улучшение.

ПРИНЯТЫЕ ОБОЗНАЧЕНИЯ

1. $(a_1, a_2, \ldots, a_n)$ и $[a_1, a_2, \ldots, a_n]$ — соответственно наибольший общий делитель (НОД) и наименьшее общее кратное (НОК) чисел a_i $(i=1, 2, 3, \ldots, n)$.

2. $\vdots$ — делится на.

3. p — простое число.

4. $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = \prod\limits_{i=1}^{k} p_i^{\alpha_i}$, где p_i — различные простые и α_i — натуральные числа, — каноническое разложение натурального числа.

5. $\overline{a_n \ldots a_1 a_0}$ — $(n+1)$-значное натуральное число, имеющее цифры a_i $(i=0, 1, 2, \ldots, n)$.

6. $\left(\frac{a}{p}\right)$ — символ Лежандра для числа a по модулю p.

7. $\frac{P_n}{Q_n} = (q_0, q_1, \ldots, q_n) = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_n}}}}$ — подходящая дробь n-го порядка.

8. $(\overline{q_0, q_1, \ldots, q_n})$ — чистая периодическая непрерывная дробь.

9. $(q_0, q_1, \ldots, q_n, \overline{b_1, b_2, \ldots, b_s})$ — смешанная периодическая непрерывная дробь с неполными частными q_i $(i=0, 1, \ldots, n)$ до первого периода.

10. $\varphi(m)$ — функция Эйлера, выражающая число натуральных чисел, не превышающих m и взаимно простых с m.

11. $[x]$ и $\{x\}$ — соответственно целая и дробная часть действительного числа x.

12. $\tau(m)$ и $\sigma(m)$ — соответственно число и сумма делителей натурального числа m.

13. $\pi(x)$ — число простых чисел, не превышающих $x>0$.

14. $(2m+1)!!$ — произведение всех нечетных натуральных чисел от 1 до $2m+1$.

15. $(2m)!!$ — произведение всех четных натуральных чисел от 1 до $2m$.

16. $P_m(a)$ — показатель, которому принадлежит число a по модулю m.

ГЛАВА I

ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ

§ 1. Теорема о делении с остатком

В теории целых чисел $(0, \pm 1, \pm 2, \ldots)$ большую роль играет теорема о делении с остатком: для любых целых чисел $a>0$ и $m>0$ существует и притом единственная пара целых чисел q и r, таких, что $a=mq+r$, $0\leqslant r<m$. При этом число a называют делимым, m — делителем или модулем, q — частным и r — остатком от деления a на m (мы ограничиваемся случаем натурального модуля, так как к нему всегда можно свести другие случаи). Если $r=0$, то говорят, что $a \vdots m$. Полезно заметить, что соотношение $a=mq+r$, $0\leqslant r<m$ может быть записано в виде $\frac{a}{m}=q+\frac{r}{m}$, $0\leqslant\frac{r}{m}<1$. Таким образом, q служит целой частью числа $\frac{a}{m}$, а $\frac{r}{m}$ — дробной его частью.

Большое применение имеет также признак делимости суммы: если $a \vdots m$ и $b \vdots m$, то и $(a+b) \vdots m$ (мы его формулируем для двух слагаемых). Важно отметить, что верна следующая обратная теорема: если $(a+b) \vdots m$ и $a \vdots m$, то и $b \vdots m$.

1. Найти частное и остаток от деления: 1) 1207 на 151; 2) 10 на 10; 3) 100 на 101; 4) -4 на 3; 5) $23_{(8)}$ на $5_{(8)}$ (в восмеричной системе счисления); 6) $123401_{(5)}$ на $13_{(5)}$; 7) $12101_{(3)}$ на $20_{(3)}$; 8) $-222_{(4)}$ на $21_{(4)}$.

2. Найти целые числа, дающие: 1) при делении на 3 частное -2; 2) при делении на $12_{(3)}$ частное $11_{(3)}$; 3) при делении на $21_{(4)}$ частное -1.

3. Найти наибольшее целое число, дающее при делении на 13 частное 17.

4. Найти модуль (делитель) и остаток, если делимое и частное соответственно равны: 1) 25 и 3; 2) -30 и -4.

5. Доказать, что: 1) квадрат нечетного натурального числа при делении на 8 дает остаток 1; 2) сумма квадратов двух последовательных натуральных чисел при делении на 4 дает остаток 1.

6. Доказать, что простое число $p \geqslant 5$ при делении на 6 дает остаток 1 или 5.

7. Доказать, что квадрат простого числа $p \geqslant 5$ при делении на 24 дает остаток 1.

8. Доказать теорему: если каждое из двух целых чисел при делении на натуральное число m дает остаток 1, то и их произведение при делении на m дает остаток 1.

9. Доказать, что числа вида $3m+2$ ($m=1, 2, \ldots$) не являются квадратами целых чисел.

10. Число $N=1441_{(q)}$ при делении на 7 дает остаток 1. Найти основание системы счисления q, если известно, что $q \leqslant 11$.

11. Методом математической индукции доказать, что любая натуральная степень 15 при делении на 7 дает остаток 1.

12. Доказать, что: 1) все числа вида $2^{2^n}+1$ ($n=2, 3, \ldots$) оканчиваются цифрой 7; 2) числа вида $2^{4n}-5$ ($n=1, 2, \ldots$) оканчиваются цифрой 1.

13. Доказать, что сумма квадратов двух нечетных чисел не является квадратом целого числа.

14. Доказать, что в пифагоровом треугольнике (прямоугольном треугольнике, стороны которого выражаются натуральными числами) по крайней мере один из катетов делится на 3.

15. Доказать, что по крайней мере одна сторона пифагорова треугольника делится на 5.

16. Найти все натуральные числа n, такие, что сумма $s_n=1+2+\ldots+n$ при делении на 5 дает остаток 1.

17. Если $ax-by \,\vdots\, m$, $a-b \,\vdots\, m$ и числа b и m не имеют общих натуральных делителей, отличных от 1, то $x-y \,\vdots\, m$. Доказать.

18. Доказать, что числа вида $4^n+15n-1$ ($n=1, 2, \ldots$) кратны 9.

19. Доказать, что значения функций $f(n)=10^n+18n-1$ и $F(n)=3^{2n+3}+40n-27$ натурального аргумента соответственно кратны 27 и 64.

20. Доказать, что дроби вида $\frac{n}{2n^2+1}$ и $\frac{n}{n^2+n+1}$ обращаются в чистую периодическую десятичную дробь.

21. Если сумма двух трехзначных чисел делится на 37, то и шестизначное число, составленное приписыван-

ем одного из них к другому, также делится на 37. Доказать.

22. Доказать, что: 1) $m^5-m \vdots 5$; 2) $m(m^2+5) \vdots 6$; 3) $m(m+1)(2m+1) \vdots 6$.

23. Зная, что $7\cdot 11\cdot 13=1001$, вывести общий признак делимости на 7, на 11 и на 13. Применить этот признак делимости к числу 368312.

24. Доказать, что разность чисел, имеющих одинаковую сумму цифр, кратна 9.

25. Доказать, что сумма $2n+1$ последовательных натуральных чисел кратна числу $2n+1$.

26. Доказать, что дробь, у которой числитель есть разность квадратов нечетных чисел, а знаменатель — сумма их квадратов, сократима на 2, но не сократима на 4.

27. Если трехзначное число делится на 37, то все числа, полученные из данного круговой перестановкой его цифр, делятся на 37. Доказать. Составить и решить аналогичную задачу относительно шестизначного числа.

28. Методом математической индукции доказать, что натуральное число, составленное из 3^n ($n=1, 2, \ldots$) одинаковых цифр, делится на 3^n.

§ 2. Наибольший общий делитель (НОД) и наименьшее общее кратное (НОК)

При решении задач этого параграфа следует иметь в виду следующие два основных свойства НОД и НОК, т. е. чисел $(a_1, a_2, \ldots, a_n)\geqslant 1$ и $[a_1, a_2, \ldots, a_n]>1$: 1) НОД данных чисел (компонентов) делится на любой их ОД и 2) любое ОК данных чисел делится на их НОК.

Рекуррентные формулы

$$(a_1, a_2, \ldots, a_{n-1}, a_n)=((a_1, a_2, \ldots, a_{n-1}), a_n)$$
$$\text{и } [a_1, a_2, \ldots, a_n]=[[a_1, a_2, \ldots, a_{n-1}], a_n]$$

позволяют вычисление НОД и НОК нескольких чисел сводить к вычислению НОД и НОК двух чисел. НОД двух чисел может быть вычислен как с помощью их канонического разложения, так и с помощью алгоритма Евклида.

Числа $a_1, a_2, \ldots, a_n$ называются взаимно простыми, если $(a_1, a_2, \ldots, a_n)=1$ и попарно взаимно простыми, если $(a_{i_1}, a_{i_2})=1$.

НОД и НОК двух чисел a и b связаны соотношением $(a, b)[a, b]=ab$, не имеющим места для большего числа компонентов.

Общий множитель компонентов можно выносить за знак НОД и НОК.

Частные от деления компонентов на их НОД являются взаимно простыми числами.

НОК данных чисел равно их произведению тогда и только тогда, когда эти числа являются попарно взаимно простыми.

29. Найти: 1) $(420, 126, 525)$ и $[420, 126, 525]$; 2) $(529, 1541, 1817)$ и $[529, 1541, 1817]$.

30. Доказать, что: 1) $[6, 35, 143]=6.35.143$; 2) $[n, n+1]=n(n+1)$.

31. Доказать, что НОД двух последовательных четных чисел равен 2, а нечетных 1.

32. Доказать, что $(cb, bc, ca) \vdots (a, b, c)^2$.

33. Если $(a, b)=1$, то $(a+b, a-b)$ равен либо 1, либо 2. Доказать.

34. Дробь $\frac{a}{b}$ несократима. Будет ли несократимой дробь $\frac{a}{a+b}$?

35. Разность двух нечетных чисел равна 2^n. Доказать, что эти числа взаимно простые.

36. Найти НОД следующих чисел: 1) $d=(a, b)$ и $m=[a, b]$; 2) ab и $m=[a, b]$; 3) $a+b$ и ab, где $(a, b)=1$; 4) $a+b$ и $m=[a, b]$.

37. Найти: 1) $(n, 2n+1)$; 2) $(10n+9, n+1)$; 3) $(3n+1, 10n+3)$.

38. Доказать, что $\left(\frac{x}{a}, \frac{x}{b}\right)=1$ тогда и только тогда, когда $x=[a, b]$.

39. Доказать, что для нечетных чисел a, b и c имеет место равенство $(a, b, c)=\left(\frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}\right)$.

40. Доказать, что $(a, b)=(5a+3b, 13a+8b)$.

41. Найти, чему могут быть равны НОД и НОК трех последовательных натуральных чисел.

42. Число nab, где n, a, b — натуральные числа и $(a, b)=1$, представить в виде $ax+by$, где x и y также натуральные числа.

43. Доказать теорему Евклида: если $(a, c)=(b, c)=$ $=1$, то $(ab, c)=1$.

44. Может ли НОД двух натуральных чисел быть больше их разности?

45. Если $(a, c)=1$, то $b \vdots (ab, c)$. Доказать.

46. Если $(a, b)=1$, то $(ac, b)=(c, b)$. Доказать.

47. Доказать, что для натуральных чисел m, n и k имеет место соотношение $mnk=[m, n, k]\cdot(mn, mk, nk)$.

48. Решить в натуральных числах следующие системы уравнений:

1) $\begin{cases} x+y=150, \\ (x, y)=30; \end{cases}$ 2)* $\begin{cases} (x, y)=45, \\ \dfrac{x}{y}=\dfrac{11}{7}; \end{cases}$ 3) $\begin{cases} xy=8400, \\ (x, y)=20; \end{cases}$

4) $\begin{cases} \dfrac{x}{y}=\dfrac{5}{9}, \\ (x, y)=28; \end{cases}$ 5) $\begin{cases} xy=20, \\ [x, y]=10. \end{cases}$

49. Доказать, что натуральное число $N=10a+b$ $(0\leqslant b\geqslant 9)$ делится на $m=10q+1$ тогда и только тогда, когда $a-bq \vdots m$.

50. Опираясь на теорему предыдущей задачи, вывести признак делимости на число, оканчивающееся семью.

51. Доказать, что натуральное число $N=10a+b$ $(0\leqslant b\leqslant 9)$ делится на $m=10q+9$ тогда и только тогда, когда $a+b(q+1) \vdots m$.

52. Опираясь на теорему предыдущей задачи, вывести признак делимости на число, оканчивающееся тремя.

53. Чтобы число $N=\overline{a_n \ldots a_1a_0}$ делилось на 19, необходимо и достаточно, чтобы на 19 делилось число $N_1=\overline{a_n \ldots a_2a_1}+2a_0$. Доказать и проследить на примерах.

§ 3. Простые и составные числа

Натуральное число называется простым, если оно имеет только два различных делителя (единицу и самого себя), и составным, если оно имеет более двух делителей. Единица не относится ни к простым, ни к составным числам. Простые числа (и их натуральные степени) являются попарно взаимно простыми. Наименьший, отличный от 1 делитель данного числа есть число простое. Всякое составное число может быть представлено в виде произведения простых чисел и притом однозначно (если представления, отличающиеся лишь порядком сомножителей, не считать различными).

54. Доказать, что нечетные числа вида $6n+1$ ($n=1, 2, \ldots$) нельзя представить как разность простых чисел.

55. Найти все нечетные числа, представимые в виде разности простых чисел.

56. Доказать, что квадрат числа $N=3m+2$ ($m=1, 2, \ldots$) не может быть представлен в виде суммы квадрата натурального числа и простого числа.

57. Доказать, что наименьший простой делитель составного числа a не превышает $\sqrt{a}$. Верна ли данная теорема в случае простого a?

58. При помощи теоремы предыдущей задачи выяснить, простыми или составными являются числа: 1) 127; 2) 919; 3) 7429.

59. Найти все простые числа между: 1) 100 и 110; 2) 190 и 200; 3) 200 и 220.

60. Доказать, что между натуральными числами n и $n!$, где $n>2$, содержится по крайней мере одно простое число.

61. Написать 12 последовательных составных натуральных чисел.

62. Доказать, что по модулю 4 множество всех простых чисел может быть разбито на два подмножества: на простые числа вида $4n+1$ и на простые числа вида $4n+3$.

63. Найти натуральные значения n, такие, чтобы числа n, $n+10$ и $n+14$ все были простыми.

64. Найти простое число p, чтобы число $2p^2+1$ было также простым.

65. Найти такое простое число p, чтобы числа $4p^2+1$ и $6p^2+1$ оба были простыми.

66. Доказать, что указанные ниже числа одновременно простыми быть не могут: 1) $p+5$ и $p+10$; 2) p, $p+2$ и $p+5$; 3) 2^n-1 и 2^n+1, где $n>2$.

67. Если числа p и $8p^2+1$ простые, то число $8p^2+2p+1$ также простое. Доказать.

68. Доказать, что 3, 5 и 7 являются единственной тройкой простых чисел-близнецов (т. е. тройкой простых

чисел, составляющих арифметическую прогрессию с разностью 2).

69. При помощи таблицы простых чисел найти наименьшее значение индекса n, при котором число вида $p_1p_2 \ldots p_n+1$, где p_i — простые числа, записанные в порядке возрастания (начиная с 2), есть число составное.

70. Доказать, что не существует наибольшего простого числа вида $3n+2$ $(n=1, 2, \ldots)$.

71. Доказать, что арифметическая прогрессия с первым членом 7 и разностью 4 содержит бесконечное множество простых чисел.

72. Доказать, что произведение всех простых чисел, не превышающих натуральное число $n>2$, больше n.

73. Доказать, что $p_{n+1}<p_1p_2 \ldots p_n$, где $p_i (i=1, 2, \ldots, n)$ — первые n простых чисел и p_{n+1} — следующее за p_n простое число.

74. Методом математической индукции доказать, что $p_n \leqslant 2^{2^{n-1}}$, где p_n — энное простое число $(p_1=2, p_2=3, \ldots \ldots)$, причем знак равенства имеет место только в случае $n=1$.

75. Доказать, что $p_n>2n$ $(n=5, 6, \ldots)$.

ГЛАВА 2

СРАВНЕНИЯ

§ 4. Понятие сравнения

Сравнимые по данному модулю числа обычно определяются как равноостаточные. Таким образом, если $a=mq_1+r$ и $b=mq_2+r$, то по определению $a\equiv b \pmod m$.

Сравнимые по данному модулю числа имеют с ним один и тот же НОД. Обратное утверждение неверно.

Чтобы данные числа были сравнимы по данному модулю, необходимо и достаточно, чтобы их разность делилась на этот модуль. Таким образом, например, $a\equiv \equiv 0 \pmod m$ является еще одним способом выражения того, что $a \vdots m$. Важно также иметь в виду, что для сравнимых по модулю m целых чисел a и b существует и притом только одно целое число q, такое, что $a=b+mq$.

76. По какому модулю все целые числа сравнимы между собой?

77. Привести примеры целых чисел, сравнимых по модулю 8.

78. Привести примеры целых чисел, имеющих с модулем 6 один и тот же НОД, но не сравнимых по этому модулю.

79. Применить понятие сравнения к доказательству того, что числа 210 и 858 имеют с модулем 12 один и тот же НОД. Применим ли этот прием относительно чисел 385 и 77 и модуля 6?

80. Какие из следующих сравнений являются верными: 1) $1\equiv -5 \pmod 6$; 2) $546\equiv 0 \pmod{13}$; 3) $2^3\equiv\equiv 1 \pmod 4$; 4) $3m\equiv -1 \pmod m$?

81. Доказать, что следующие сравнения являются верными: 1) $121\equiv 13145 \pmod 2$; 2) $121347\equiv 92817 \pmod{10}$; 3) $31\equiv -9 \pmod{10}$; 4) $(m-1)^2\equiv 1 \pmod m$; 5) $2m+1\equiv (m+1)^2 \pmod m$.

82. Доказать, что следующие сравнения являются неверными: 1) $5^{1812}\equiv 1964 \pmod{25}$; 2) $7^{103}\equiv 3 \pmod{27}$; 3) $4^{1965}\equiv 25 \pmod{10}$; 4) $30\cdot 17\equiv 81.19 \pmod 6$;

5) $(2n+1)(2m+1)\equiv 2k \pmod 6$, где n, m и k — числа целые.

83. Доказать, что каждое целое число сравнимо со своим остатком по данному модулю.

84. Число x удовлетворяет условию $x\equiv 2 \pmod{10}$. Записать это условие в виде уравнения с параметром и найти несколько значений x.

85. Найти все значения x, удовлетворяющие сравнениям: 1) $x\equiv 0 \pmod 3$; 2) $x\equiv 1 \pmod 2$.

86. Найти значения m, удовлетворяющие условию: 1) $20\equiv 8 \pmod m$; 2) $3p+1\equiv p+1 \pmod m$.

87. Указать возможные значения модуля в сравнении $x\equiv 5 \pmod m$, если известно, что этому сравнению удовлетворяет $x=13$.

§ 5. Основные свойства сравнений

К основным свойствам сравнений относятся следующие:

1. Каждое целое число сравнимо с самим собой по любому модулю (рефлексивность или закон тождества).
2. Части сравнения можно менять местами (симметрия).
3. Числа, сравнимые с одним и тем же числом, сравнимы между собой по данному модулю (транзитивность)
4. Сравнения по одному и тому же модулю можно почленно складывать, вычитать и перемножать.

Это свойство имеет следующие следствия: к частям (из частей) сравнения можно прибавлять (вычитать) одно и то же число; части сравнения можно умножать на одно и то же число, а также возводить в одну и ту же натуральную степень; к любой (из любой) части сравнения можно прибавлять (вычитать) число, кратное модулю.

5. Части сравнения можно делить на их общий делитель, взаимно простой с модулем.
6. Части сравнения и модуль можно делить (умножать) на одно и то же число.
7. Если числа сравнимы по данному модулю, то они сравнимы по модулю-делителю данного модуля.
8. Если числа сравнимы по нескольким модулям, то они сравнимы по модулю — НОК данных модулей.

88. Доказать, что сравнимым по данному модулю значениям аргументов соответствуют сравнимые значения

полинома $F(x, y, z)=ax^3+bx^2y+cxyz+dz$ с целыми коэффициентами.

89. Если $3^n\equiv-1 \pmod{10}$, где n — число натуральное, то $3^{n+4}\equiv-1 \pmod{10}$. Доказать.

90. Доказать, что $2^{5n}-1 \vdots 31$, где n — число натуральное.

91. Доказать, что $1+3^x+9^x \vdots 13$, если $x=3n+1$ $(n=0, 1, 2, \ldots)$.

92. Доказать, что $(a+b)^p\equiv a^p+b^p \pmod p$.

93. Доказать, что $a^p\equiv b^p \pmod{p^{n+1}}$, если $a\equiv b \pmod{p^n}$.

94. Доказать, что сравнения по одному и тому же модулю можно почленно делить, если части сравнения-делителя являются числами взаимно простыми с модулем. Вывести отсюда правило о делении частей сравнения на число, взаимно простое с модулем.

95. Доказать, что если $ax\equiv bx \pmod m$, то $a\equiv b\left(\bmod \dfrac{m}{(x, m)}\right)$.

96. Если $\overline{a_4a_3a_2a_1a_0}\equiv0 \pmod{33}$, то $a_4+\overline{a_3a_2}+\overline{a_1a_0}\equiv0 \pmod{33}$. Доказать. При $a_{i+1}=0$ считать $\overline{a_{i+1}a_i}=a_i$.

97. Исходя из $p-i\equiv-i \pmod p$ где $i=1, 2, \ldots, n$, доказать, что: 1) $C_{p-1}^n\equiv(-1)^n \pmod p$; 2) $C_{p-2}^n\equiv(-1)^n(n+1) \pmod p$.

98. Найти последние две цифры чисел: 1) 9^{9^9}; 2) 7^{9^9}.

99. Доказать, что $p^{p+2}+(p+2)^p\equiv0 \pmod{2p+2}$, где $p>2$.

100. Доказать, что числа

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2}$$

попарно несравнимы по модулю $p>2$.

101. Исходя из $i\equiv i-m \pmod m$, доказать, что $\sum\limits_{i=1}^{m} i^n\equiv0 \pmod m$, где n и m — числа нечетные.

102. Доказать, что $2^{3^n}\equiv-1 \pmod{3^{n+1}}$, где $n=1, 2, 3, \ldots$.

103. При помощи сравнения предыдущей задачи доказать, что существует бесконечное множество натуральных чисел $m>1$, удовлетворяющих условию $2^m+1\equiv0 \pmod m$.

104. Доказать, что $(m-1)^{m^n}\equiv-1 \pmod{m^{n+1}}$, где $m>1$ — число нечетное и n — натуральное.

105. При помощи сравнения предыдущей задачи доказать, что существует бесконечное множество натуральных чисел x, удовлетворяющих условию $2^{2x}+1\equiv 0 \pmod x$.

106. Доказать, что числа вида $N=3^{2^{4n+1}}+2$ и вида $M=2^{3^{4n+1}}+3$, где $n=1, 2, \ldots$, являются составными.

107. Доказать, что уравнения $2^x+7^y=19^z$ и $2^x+5^y=19^z$ не имеют решения в натуральных числах.

108. Доказать, что число вида $\frac{18a+5b}{19}$ есть целое, если известно, что число вида $\frac{11a+2b}{19}$ является целым (числа a и b — целые).

§ 6. Классы по данному модулю

По модулю m существует m классов сравнимых чисел. Числа данного класса называют вычетами относительно друг друга.

Система чисел, взятых по одному из каждого класса, называется полной системой вычетов по данному модулю. Каждому модулю соответствует бесконечное множество полных систем вычетов, простейшей из которых является полная система остатков: $0, 1, 2, \ldots, m-1$. Система целых чисел $x_1, x_2, \ldots, x_s$ тогда и только тогда является полной системой вычетов по модулю m, когда $s=m$ и $x_{i_1} \not\equiv x_{i_2} \pmod m$. Чтобы значения линейной формы $ax+b$, где $(a, m)=1$, пробегали полную систему вычетов по модулю m, необходимо и достаточно, чтобы соответствующие значения x пробегали полную систему вычетов по модулю m.

Система чисел, взятых по одному из каждого класса вычетов, взаимно простых с модулем, называется приведенной системой вычетов по данному модулю. Из бесконечного множества приведенных систем вычетов по данному модулю простейшей является приведенная система остатков. Каждая приведенная система вычетов содержит столько вычетов, сколько существует натуральных чисел, не превосходящих m (модуль) и взаимно простых с m. Эту функцию от m (функцию Эйлера или φ-функцию) обычно обозначают $\varphi(m)$. Система чисел $x_1, x_2, \ldots, x_s$ тогда и только тогда является приведенной системой вычетов по модулю m, когда $s=\varphi(m)$,

$x_{i_1} \not\equiv x_{i_2} \pmod m$ и $(x_i, m) = 1$. Чтобы значения формы ax, где $(a, m) = 1$, пробегали приведенную систему вычетов по модулю m, необходимо и достаточно, чтобы соответствующие значения x пробегали приведенную систему вычетов по модулю m.

109. Записать в виде сравнений все классы по модулю 10.

110. Записать все классы по модулю 10 при помощи формулы $x = 10q + r$, $0 \leqslant r < 10$.

111. Указать все классы вычетов: 1) взаимно простых с модулем 10; 2) имеющих с модулем 10 НОД, равный 2; 3) имеющих с модулем 10 НОД, равный 5; 4) имеющих с модулем 10 НОД, равный 10.

112. Доказать, что каждый класс по модулю m состоит из d классов по модулю md.

113. Убедиться в том, что множество классов по модулю 10 есть кольцо относительно их сложения и умножения (которые определяются через сложение и умножение произвольных вычетов классов-компонентов).

114. Найти несколько полных систем вычетов по модулю 10.

115. По какому модулю числа 20, —4, 22, 18, —1 составляют полную систему вычетов?

116. Доказать, что система чисел 20, 31, —8, —5, 25, 14, 8, —1, 13 и 6 не является полной системой вычетов по модулю 10.

117. Доказать, что любые m последовательных целых чисел составляют полную систему вычетов по модулю m.

118. Доказать, что числа $-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}$ составляют полную систему вычетов по нечетному модулю m.

119. Найти хотя бы одну полную систему вычетов вида $3x-1$ по модулю 10.

120. Найти хотя бы одну полную систему вычетов вида $5x$ по модулю 4.

121. Если числа вида $ax_i + b$ $(i = 1, 2, \ldots, m)$ составляют полную систему вычетов по модулю m, то и соответствующие числа x_i также составляют полную систему вычетов по модулю m. Доказать.

122. Если числа вида $a_n x_i^n + \ldots + a_1 x_i + a_0$ $(i = 1, 2, \ldots, m)$ составляют полную систему вычетов по модулю m, то и соответствующие числа x_i также составляют полную систему вычетов по модулю m и наоборот. Доказать.

123. Написать несколько приведенных систем вычетов по модулю 6.

124. Почему система чисел $-5, 13, 11, -21, 5$ не является приведенной системой вычетов по модулю 12?

125. Доказать, что приведенная система вычетов по модулю p состоит из $p-1$ вычетов.

126. Доказать, что система чисел $-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, \ldots, -1, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2}$ является приведенной системой вычетов (наименьших по абсолютной величине) по модулю $p>2$.

127. Доказать, что система чисел $5, 5^2, 5^3, 5^4, 5^5, 5^6$ является приведенной системой вычетов по модулю 7.

128. Если числа вида ax_i ($i=1, 2, \ldots, \varphi(m)$) составляют приведенную систему вычетов по модулю m, то соответствующие числа x_i также составляют приведенную систему вычетов по модулю m и наоборот. Доказать.

129. Доказать теорему: если $(a, m)=1$, $b\equiv 0 \pmod{m}$ и значения x составляют приведенную систему вычетов по модулю m, то и соответствующие значения функции $ax+b$ также составляют приведенную систему вычетов по модулю m.

130. Доказать теорему: если $(a, m)=d$ и значения x составляют полную систему вычетов по модулю $\frac{m}{d}$, то и соответствующие значения функции $\frac{a}{d}x+b$ также составляют полную систему вычетов по модулю $\frac{m}{d}$.

131. Доказать теорему: если $(a, m)=d$ и значения x составляют приведенную систему вычетов по модулю $\frac{m}{d}$, то и соответствующие значения функции $\frac{a}{d}x$ также составляют приведенную систему вычетов по модулю $\frac{m}{d}$.

§ 7. Функция Эйлера

Как уже отмечалось, функция Эйлера $\varphi(m)$ выражает число натуральных чисел, не превышающих m и взаимно простых с m. Существует $\varphi(m)$ классов вычетов, взаимно простых с модулем m. Условились считать $\varphi(1)=1$.

Если $m>1$ имеет каноническое разложение $\prod_{i=1}^{k} p_i^{\alpha_i}$, то

$$\varphi(m)=m\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \text{ или } \varphi(m)=\prod_{i=1}^{k} p_i^{\alpha_i-1}\cdot\prod_{i=1}^{k}(p_i-1).$$

Функция Эйлера мультипликативна, т.е. если $(m_{i_1}, m_{i_2})=$ $=1$, то $\varphi\left(\prod_{i=1}^{n} m_i\right)=\prod_{i=1}^{n}\varphi(m_i)$.

132. Представить графически изменение функции $\chi=\varphi(x)$, где x — число натуральное (функции Эйлера).

133. Вычислить: 1) $\varphi(1000)$; 2) $\varphi(125)$; 3) $\varphi(180)$; 4) $\varphi(360)$; 5) $\varphi(1001)$.

134. Найти число классов вычетов, взаимно простых с модулем 1225.

135. Сколько существует положительных правильных несократимых дробей со знаменателем m?

136. Сколько натуральных чисел в промежутке от 1 до 120, не взаимно простых с 30?

137. Найти число классов вычетов, имеющих с модулем m НОД, равный d. Сколько существует классов вычетов, имеющих с модулем 10 НОД, равный 2?

138. Вывести формулы: 1) $\varphi(2^\alpha)=2^{\alpha-1}$; 2) $\varphi(p^\alpha)=$ $=p^{\alpha-1}\varphi(p)$; 3) $\varphi(m^\alpha)=m^{\alpha-1}\varphi(m)$. Число α — натуральное.

139. Доказать, что $\varphi(2m)$ может быть равно либо $\varphi(m)$, либо $2\varphi(m)$. Найти критерий для каждого из этих случаев.

140. Доказать справедливость следующих равенств:

1) $\varphi(4n+2)=\varphi(2n+1)$;

2) $\varphi(4n)=\begin{cases} 2\varphi(n) & \text{при } (n, 2)=1, \\ 2\varphi(2n) & \text{при } (n, 2)=2. \end{cases}$

141. Решить уравнения 1) $\varphi(5^x)=100$; 2) $\varphi(7^x)=$ $=294$; 3) $\varphi(p^x)=p^{x-1}$; 4) $\varphi(3^x\cdot 5^x)=600$. Числа x и y натуральные.

142. Доказать, что при $m\geqslant 3$ значение $\varphi(m)$ — число четное.

143. Если уравнение $\varphi(x)=a$ имеет корень $x=m$, где $(m, 2)=1$, то оно имеет также корень $x=2m$. Доказать.

144. Известно, что $(m, n)>1$. Что больше: $\varphi(mn)$ или $\varphi(m)\varphi(n)$?

145. Доказать, что $\varphi(mn)=\varphi(m)\varphi(n)\cdot\frac{d}{\varphi(d)}$, где $d=(m, n)$.

146. Доказать, что $\varphi(mn)=\varphi(\delta)\varphi(\mu)$, где $\delta=(m, n)$ и $\mu=[m, n]$.

147. Чему равна сумма $\varphi(1)+\varphi(p)+\varphi(p^2)+\ldots+\varphi(p^\alpha)$, где α — число натуральное?

148. Чему равна сумма $\varphi\left(\frac{m}{d_1}\right)+\varphi\left(\frac{m}{d_2}\right)+\ldots+\varphi\left(\frac{m}{d_k}\right)$, где d_i — все натуральные делители модуля m?

149. Доказать тождество Гаусса: $\varphi(d_1)+\varphi(d_1)+\ldots$ $\ldots+\varphi(d_k)=m$, где d_i — все натуральные делители m.

150. Вывести формулу для суммы натуральных чисел, не превышающих m и взаимно простых с m.

151. Доказать, что сумма натуральных чисел, не превышающих p и взаимно простых с p, в два раза меньше числа натуральных чисел, не превышающих p^2 и взаимно простых с p^2.

152. По какому модулю числа 1 и 5 составляют приведенную систему вычетов?

153. По какому модулю существует 4 класса вычетов, взаимно простых с этим модулем?

154. Решить уравнения: 1) $\varphi(x)=2^x$; 2) $\varphi(p^x)=6\cdot p^{x-2}$.

155. Решить уравнения: 1) $\varphi(x)=p-1$; 2) $\varphi(x)=14$; 3) $\varphi(x)=8$; 4) $\varphi(x)=12$.

156. Решить уравнение $\varphi(m)=3600$, где $m=3^\alpha 5^\beta 7^\gamma$.

157. Решить уравнение $\varphi(x)=120$, где $x=p_1p_2$ и $p_1-p_2=2$.

158. Решить уравнение $\varphi(m)=11424$, где $m=p_1^2p_2^2$.

159. Исследовать уравнения: 1) $\varphi(x)=\varphi(px)$; 2) $\varphi(px)=p\varphi(x)$; 3) $\varphi(p_1x)=\varphi(p_2x)$. Числа p_1 и p_2 различные простые.

160. Решить уравнения: 1) $\varphi(x)=\frac{x}{2}$; 2) $\varphi(x)=\frac{x}{3}$; 3) $\varphi(x)=\frac{x}{4}$.

161. Исследовать уравнение $\varphi(p^x)=a$.

162. При помощи свойств функции Эйлера доказать бесконечность множества всех простых чисел.

163. Найти число размещений с повторениями из m первых натуральных чисел по n таких, НОД которых взаимно прост с m (обобщение функции Эйлера).

§ 8. Теорема Эйлера

Чтобы $a^{\varphi(m)} \equiv 1 \pmod{m}$, необходимо и достаточно, чтобы $(a, m) = 1$.

164. Доказать, что цифра единиц 12-й степени натурального числа, каноническое разложение которого не содержит множителей 2 и 5, есть 1.

165. Доказать, что: 1) $a^{12}-1 \vdots 7$, если $(a, 7)=1$; 2) $a^{12}-b^{12} \vdots 65$, если $(a, 65)=(b, 65)=1$.

166. Доказать, что число вида $a^{p-1}+p-1$, где $a \not\equiv 0 \pmod{p}$, является составным.

167. Доказать, что $\sum\limits_{i=1}^{p-1} i^{k(p-1)}+1 \equiv 0 \pmod{p}$.

168. Доказать, что $2^{11\cdot 31} \equiv 2 \pmod{11\cdot 31}$.

169. Доказать, что $\left(\sum\limits_{i=1}^{n} a_i\right)^p \equiv \sum\limits_{i=1}^{n} a_i^p \pmod{p}$.

170. Доказать, что $a^{n(p-1)+1} \equiv a \pmod{p}$.

171. Доказать, что наименьшее натуральное значение x, удовлетворяющее сравнению $a^x \equiv 1 \pmod{m}$, где $(a, m)=1$, является делителем числа $\varphi(m)$.

172. Доказать, что $a^{561} \equiv a \pmod{11}$.

173. Доказать, что сравнению $x^{(p-1)m}+x^{(p-1)n} \equiv 0 \pmod{p}$ может удовлетворять только значение x, кратное $p>2$.

174. Доказать, что натуральное число m, не делящееся ни на 2, ни на 3, ни на 5, является делителем $\varphi(m)$-значного числа вида $11\ldots 1$.

175. Доказать, что: 1) $a^{560} \equiv 1 \pmod{561}$, где $(a, 561)=1$; 2) $2^{1093\cdot 1092} \equiv 1 \pmod{1093^2}$.

176. Доказать, что при любом целом значении x: 1) $x^7 \equiv x \pmod{42}$; 2) $x^{13} \equiv x \pmod{2730}$.

177. Найти остаток от деления сотой степени целого числа на 125.

178. Доказать теорему: если $\sum\limits_{i=1}^{n} a_i \equiv 0 \pmod{30}$, то $\sum a_i^5 \equiv 0 \pmod{30}$.

179. Доказать, что $p_1^{p_2-1}+p_2^{p_1-1}\equiv 1 \pmod{p_1p_2}$, где p_1 и p_2 — различные простые числа.

180 Если $2p+1$ $(p\neq 3)$ — число простое, то $4p+1\equiv\equiv 0 \pmod 3$. Доказать.

181. Если $(a, m)=1$ и $\alpha_1\equiv\alpha_2 \pmod{\varphi(m)}$, то $a^{\alpha_1}\equiv\equiv a^{\alpha_2} \pmod m$. Доказать.

182. Найти значение p из условия $5^{p^2}+1\equiv 0 \pmod{p^2}$.

183. Найти остаток от деления $2^{\varphi(m)-1}$на нечетное число m.

184. При помощи теоремы Эйлера найти значение x, удовлетворяющее сравнению $ax+b\equiv 0 \pmod m$, где $(a, m)=1$.

§ 9. Алгебраические сравнения с одним неизвестным

Решить алгебраическое сравнение энной степени с неизвестным x, т. е. сравнение $a_nx^n+\ldots+a_2x^2+a_1x+a_0\equiv\equiv 0 \pmod m$, где $a_n\not\equiv 0 \pmod m$, — значит найти все значения неизвестного, ему удовлетворяющие, или доказать, что таковых не существует. Решением данного сравнения называется класс чисел, ему удовлетворяющих. Общий вид решения: $x\equiv x_0 \pmod m$, где x_0 — одно из значений неизвестного, удовлетворяющее данному сравнению. Два сравнения, содержащие одно и то же неизвестное (одни и те же неизвестные), называются равносильными, если их решения выражают одно и то же множество целых чисел (в частности, пустое). Например, сравнения $2x+4\equiv 0 \pmod 6$ и $x+2\equiv 0 \pmod 3$ равносильны, так как решения $x\equiv 1; 4 \pmod 6$ первого и решение $x\equiv 1 \pmod 3$ второго выражают одно и то же множество целых чисел. Сравнение, равносильное данному, получается в результате следующих преобразований:

1) прибавления к частям данного сравнения одного и того же числа;

2) прибавления к любой части сравнения числа, кратного модулю;

3) умножения (деления) частей данного сравнения на число, взаимно простое с модулем;

4) деления частей сравнения и модуля на одно и то же число.

Сравнение по модулю-делителю данного модуля является сравнением-следствием данного сравнения. В соответствии с этим, например, чтобы решить сравнение $x^2-5x+6\equiv 0 \pmod 9$, достаточно решить сравнение-следствие $x^2-5x+6\equiv 0 \pmod 3$ или $x^2+x\equiv 0 \pmod 3$ и найденные классы значений неизвестного $x\equiv 0;\ 3;\ 6;\ 2;\ 5;\ 8 \pmod 9$ проверить по данному сравнению; данное сравнение имеет два решения: $x\equiv 2;\ 3 \pmod 9$.

Сравнение n-ой степени по простому модулю может иметь не более n решений. Сравнение первой степени, т. е. сравнение $ax\equiv b \pmod m$, при $(a, m)=1$ имеет в точности одно решение. Это решение может быть найдено путем испытания полной системы вычетов или по формуле $x\equiv b\cdot a^{\varphi(m)-1} \pmod m$ или путем преобразований с помощью основных теорем о равносильности сравнений. Если $(a, m)=d$ и $b\not\equiv 0 \pmod d$, то сравнение $ax\equiv b \pmod m$ не имеет решений. При $b\equiv 0 \pmod d$ оно имеет d решений по данному модулю $x\equiv x_0;\ x_0+\frac{m}{d},\ x_0+\frac{2m}{d};\ \ldots;\ x_0+\frac{(d-1)m}{d}\left(\bmod \frac{m}{d}\right)$, где x_0 — значение x, удовлетворяющее сравнению $\frac{a}{d}x\equiv\frac{b}{d}\left(\bmod \frac{m}{d}\right)$.

185. Непосредственным испытанием системы остатков найти все решения сравнений: 1) $2x+5\equiv 0 \pmod 3$; 2) $x^2-2x+1\equiv 0 \pmod 4$; 3) $27x^2-13x+11\equiv 0 \pmod 5$.

186. Убедиться в том, что следующие сравнения не имеют решений: 1) $2x-3\equiv 0 \pmod 6$; 2) $x^2-2x+3\equiv 0 \pmod 4$; 3) $x^3+x+4\equiv 0 \pmod 5$; 4) $x^4+2\equiv 0 \pmod 5$; 5) $x^5-2x^3+13x-1\equiv 0 \pmod 4$.

187. Убедиться в том, что следующим сравнениям удовлетворяют любые целые значения неизвестного: 1) $x^2-x+6\equiv 0 \pmod 2$; 2) $x(x^2-1)\equiv 0 \pmod 6$; 3) $x^4+2x^3-x^2-2x\equiv 0 \pmod 4$; 4) $x^p-x\equiv 0 \pmod p$.

188. При каких целых значениях x трехчлен $5x^2+x+4$ делится на 10?

189. Решить сравнение $x^2-4x+3\equiv 0 \pmod 6$, используя необходимое условие $x^2-4x+3\equiv 0 \pmod 2$.

190. Решить сравнение $x^{\varphi(30)}\equiv 1 \pmod{30}$.

191. Сколько решений имеет сравнение $x^{\varphi(m)}\equiv 1 \pmod m$?

Решить сравнение $x^{p-1}\equiv 1 \pmod p$.

192. Доказать теорему: если $b_i\equiv a_i \pmod m$, то сравнения $\sum_{i=0}^{n} b_i x^{n-i}\equiv 0 \pmod m$ и $\sum_{i=0}^{n} a_i x^{n-i}\equiv 0 \pmod m$ равносильны (в частности, любой коэффициент можно заменять числом, сравнимым с ним по данному модулю).

193. Доказать теорему: если сравнение $ax\equiv 1 \pmod m$, где $(a, m)=1$, имеет решение $x\equiv x_0 \pmod m$, то сравнение $ax\equiv b \pmod m$ имеет решение $x\equiv bx_0 \pmod m$.

194. Найти все сравнения второй степени с наименьшими неотрицательными коэффициентами, не имеющие решений по модулю 2. Решить такую же задачу относительно модуля 3.

195. Доказать теорему: сравнение $\Phi(x)\equiv 0 \pmod p$ степени $n\geqslant p$ равносильно сравнению $R(x)\equiv 0 \pmod p$, где $R(x)$ — остаток от деления $\Phi(x)$ на x^p-x.

196. Применить теорему предыдущей задачи к решению сравнений:

1) $x^5+2x^4-2x^3-2x^2+2x-1\equiv 0 \pmod 3$;
2) $x^6+x^5-2x^2-x\equiv 0 \pmod 5$;
3) $x^7-3x^6+x^5-x^3+4x^2-4x+2\equiv 0 \pmod 5$;
4) $x^{12}+x^{11}-x^2-1\equiv 0 \pmod{11}$;
5) $x^{14}-x^{13}-x^2+2x+1\equiv 0 \pmod{13}$.

197. Доказать, что сравнение $\sum\limits_{i=0}^{n} a_i x^{n-i}\equiv 0 \pmod p$, где $a_0\not\equiv 0 \pmod p$, $n-i\geqslant p$ $(i=0, 1, \ldots, k<n)$ и $n-i=pq_i+r_i$ $(0\leqslant r_i<p)$, равносильно сравнению $\sum\limits_{i=0}^{k} a_i x^{q_i+r_i}+\sum\limits_{i=k+1}^{n} a_i x^{n-i}\equiv 0 \pmod p$.

198. Применить теорему предыдущей задачи к решению сравнений: 1) $x^8-x+1\equiv 0 \pmod 3$; 2) $x^{10}+x^8+x^7-x^4-x^2+4x-3\equiv 0 \pmod 7$; 3) $x^{12}-2x^7+x^3+1\equiv 0 \pmod 5$.

199. Решить сравнения первой степени с одним неизвестным: 1) $29x\equiv 1 \pmod{17}$; 2) $21x+5\equiv 0 \pmod{29}$; 3) $7x\equiv 15 \pmod 9$; 4) $7x\equiv 9 \pmod{10}$; 5) $(a+b)x\equiv a^2+b^2 \pmod{ab}$; 6) $(a^2+b^2)x\equiv a-b \pmod{ab}$; 7) $(a+b)^2x\equiv a^2-b^2 \pmod{ab}$; 8) $2x\equiv 1+p \pmod p$, где $p>2$. В сравнениях 5) — 7) считать, что $(a, b)=1$.

200. Решить сравнения первой степени с одним неизвестным: 1) $72x\equiv 2 \pmod{10}$; 2) $8x\equiv 20 \pmod{12}$; 3) $6x\equiv 27 \pmod{12}$; 4) $10x\equiv 15 \pmod{35}$; 5) $(m-1)x\equiv 1 \pmod m$; 6) $(m+1)^2x\equiv a \pmod m$; 7) $ax\equiv 1 \pmod p$, $(a, p)=1$; 8) $(a+1)x\equiv a^2-1 \pmod m$.

201. Убедиться в том, что каждое целое число удовлетворяет по крайней мере одному из сравнений:

$x\equiv 0 \pmod 2$, $x\equiv 0 \pmod 3$, $x\equiv 1 \pmod 4$, $x\equiv 1 \pmod 6$, $x\equiv 11 \pmod{12}$.

202. Решить в целых числах уравнения: 1) $5x+4y=3$; 2) $17x+13y=1$; 3) $91x-28y=35$; 4) $2x+3y=4$; 5) $4x-3y=2$.

203. При каких наименьших натуральных значениях a и b уравнение $ax-by=31$ имеет решение $x=5$, $y=9$?

204. На прямой $8x-13y+6=0$ найти число целых точек, лежащих между прямыми $x=-100$ и $x=150$.

205. Доказать, что внутри прямоугольника, ограниченного прямыми $x=-2$, $x=5$ и $y=-1$, $y=2$, на прямой $3x-7y-1=0$ не лежит ни одной целой точки.

206. Доказать, что любое натуральное число $n>ab$, где $(a, b)=1$, может быть представлено в виде $ax+by$, где x и y — числа натуральные. Может ли быть представлено в указанном виде число $n=ab$ при данных условиях?

207. При каких целых значениях x следующие функции принимают целочисленные значения: 1) $f(x)=\frac{9x-1}{7}$; 2) $F(x)=\frac{7x-1}{15}$?

208. Доказать, что дробь $\frac{2n+1}{n(n+1)}$, где $n=2, 3, \ldots$, можно представить в виде суммы положительных дробей со знаменателями n и $n+1$.

209. Какие две цифры следует приписать к числу 32, чтобы полученное четырехзначное число делилось на 3 и на 7?

210. Для перевозки зерна имеются мешки по 60 *кг* и по 80 *кг*. Сколько нужно тех и других мешков для перевозки 440 *кг* зерна?

211. Сколько билетов по 30 коп. и по 50 коп. можно купить на 14 руб. 90 коп.?

212. Сколько почтовых марок по 3 коп. и по 4 коп. можно купить на 50 коп.?

213. На станцию прибыло 500 *т* угля в 18 вагонах. В вагонах было по 15, 20 и 30 *т* угля. Сколько вагонов было по 15, сколько по 20 и сколько по 30 *т*?

214. Найти x, если:

1) $\begin{cases} x^{100}\equiv 2 \pmod{73}, \\ x^{101}\equiv 69 \pmod{73}; \end{cases}$ 2) $\begin{cases} x^{10}\equiv 20 \pmod{29}, \\ x^{11}\equiv 13 \pmod{29}. \end{cases}$

215. Доказать, что сравнение $\sum_{i=0}^{n} a_i x^{n-i} \equiv 0 \pmod{m}$, где $(a_0, m)=1$, всегда может быть заменено равносильным сравнением вида

$$x^n + \sum_{i=1}^{n} b_i x^{n-i} \equiv 0 \pmod{m}.$$

216. Доказать, что при помощи подстановки $x=y+t$ сравнение $\sum_{i=0}^{n} a_i x^{n-i} \equiv 0 \pmod{m}$, где $(na_0, m)=1$, всегда может быть приведено к сравнению $a_0 y^n + \sum_{i=2}^{n} b_i y^{n-i} \equiv 0 \pmod{m}$.

217. При помощи сравнения $x^{p-1}-1 \equiv 0 \pmod{p}$ доказать справедливость сравнения Вильсона: $(p-1)!+1 \equiv 0 \pmod{p}$.

218. Доказать справедливость сравнений: 1) $a^p + a(p-1)! \equiv 0 \pmod{p}$; 2) $a^p \cdot (p-1)! + a \equiv 0 \pmod{p}$.

219. Доказать теорему Лейбница (следствие теоремы Вильсона): чтобы $p>2$ было числом простым, необходимо и достаточно, чтобы $(p-2)!-1 \equiv 0 \pmod{p}$.

220. При помощи сравнения Вильсона (см. задачу 217) доказать теорему Клемента: числа p и $p+2$ являются простыми числами-близнецами тогда и только тогда, когда $4[(p-1)!+1]+p \equiv 0 \pmod{p^2+2p}$.

221. При помощи сравнения Вильсона доказать, что сравнение $x^2+1 \equiv 0 \pmod{p=4k+1}$ имеет решения $x \equiv \pm(2k)! \pmod{p}$. Решить сравнение $x^2+1 \equiv 0 \pmod{13}$.

222. Доказать, что сравнение $x^n \equiv 1 \pmod{p}$ имеет n решений, если $p \equiv 1 \pmod{n}$.

223. Доказать теорему: если $f(x)=\varphi(x)\psi(x)$, где коэффициенты всех полиномов — целые числа, и если сравнение $f(x) \equiv 0 \pmod{p}$ имеет столько решений, сколько единиц в его степени, то каждое из сравнений $\varphi(x) \equiv 0 \pmod{p}$ и $\psi(x) \equiv 0 \pmod{p}$ имеет столько решений, сколько единиц в его степени.

224. Доказать, что каждое из сравнений $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ и $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, где $p>2$, имеет ровно $\frac{p-1}{2}$ решений.

225. Доказать теорему: чтобы сравнение $f(x)\equiv 0 \pmod p$, где $f(x)=x^n+\sum\limits_{i=1}^{n} a_i x^{n-i}$ и $n<p$, имело n решений, необходимо и достаточно, чтобы все коэффициенты остатка от деления x^p-x на $f(x)$ были кратными p.

226. Применить теорему предыдущей задачи к решению сравнений: 1) $x^2+2x+2\equiv 0 \pmod 5$; 2) $3x^3-4x^2-2x-4\equiv 0 \pmod 7$.

227. Решить сравнения: 1) $f(x)\equiv 0 \pmod 9$; 2) $f(x)\equiv 0 \pmod{25}$, если $f(x)=x^3+2x+3$.

228. Доказать, что сравнение $x^2\equiv a \pmod 4$, где $(a, 2)=1$, имеет решение тогда и только тогда, когда $a\equiv 1 \pmod 4$. Найти все решения данного сравнения при $a\equiv 1 \pmod 4$.

229. Доказать, что сравнение $x^2\equiv a \pmod 8$, где $(a, 2)=1$, имеет решение тогда и только тогда, когда $a\equiv 1 \pmod 8$. Найти все решения данного сравнения при $a\equiv 1 \pmod 8$.

230. Доказать, что сравнение $x^2\equiv a \pmod{2^\alpha}$, где $(a, 2)=1$ и $\alpha\geqslant 3$, имеет решение тогда и только тогда, когда $a\equiv 1 \pmod 8$.

231. Доказать, что сравнение $x^2\equiv a \pmod{2^\alpha}$, где $(a, 2)=1$ и $\alpha\geqslant 3$, имеет 4 решения.

232. Доказать, что сравнение $x^2\equiv a \pmod 9$, где $(a, 3)=1$, имеет решение тогда и только тогда, когда $a\equiv 1 \pmod 3$.

233. Найти значения a, при которых сравнение $x^2\equiv a \pmod{25}$ имеет решение.

234. Решить сравнение $x^2\equiv 17 \pmod{32}$.

235. Доказать, что сравнение $x^2\equiv -p \pmod{p^2}$ неразрешимо.

§ 10. Системы сравнений первой степени с одним неизвестным

Если каждое сравнение системы

$$\begin{cases} a_1x\equiv b_1 \pmod{\mu_1}, \\ a_2x\equiv b_2 \pmod{\mu_2}, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_kx\equiv b_k \pmod{\mu_k} \end{cases}$$

разрешимо, то она может быть приведена к простейшему виду

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x \equiv c_k \pmod{m_k}. \end{cases} \qquad (1)$$

Например, система

$$\begin{cases} 3x \equiv 6 \pmod{15}, \\ 4x \equiv 0 \pmod{6}, \\ 6x \equiv 2 \pmod{7} \end{cases}$$

приводится к системе

$$\begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 0 \pmod{3}, \\ x \equiv 5 \pmod{7}. \end{cases} \qquad (1')$$

Система (1) либо не имеет решений, либо имеет одно решение по модулю, равному НОК данных модулей. Чтобы система (1) имела решение, необходимо и достаточно, чтобы свободные члены c_i были попарно сравнимы по модулям, равным НОД соответствующих данных модулей, т. е. чтобы $c_{i_1} = c_{i_2} \pmod{(m_{i_1}, m_{i_2})}$. Таким образом, если данные модули m_i попарно взаимно просты, система (1) имеет решение по модулю, равному произведению данных модулей. Так, решение системы (1′) есть $x \equiv 12 \pmod{105}$. Действительно, из 3-го сравнения имеем: $x = 5 + 7t$; подставляя эти значения x в 1-е сравнение, получаем сравнение относительно t и находим, что $t = 1 + 5t_1$; таким образом, системе 3-го и 1-го данных сравнений удовлетворяют $x = 5 + 7(1 + 5t_1) = 12 + 35t_1$; подставляя во 2-е данное сравнение, получаем сравнение относительно t_1 и находим, что $t_1 = 3t_2$; значит, системе (1′) удовлетворяют $x = 12 + 35 \cdot 3t_2 = 12 + 105t_2$ или $x \equiv 12 \pmod{105}$. К системе сравнений первой степени могут быть приведены сравнения по составному модулю, а также системы сравнений степени выше первой с одним неизвестным.

Могут быть рассмотрены системы сравнений с несколькими неизвестными (см. задачи в конце данного параграфа).

236. Решить системы сравнений:

1) $\begin{cases} x\equiv 2 \pmod 5, \\ x\equiv 8 \pmod{11}; \end{cases}$ 2) $\begin{cases} x\equiv 7 \pmod{33}, \\ x\equiv 3 \pmod{63}; \end{cases}$ 3) $\begin{cases} 4x\equiv 3 \pmod 7, \\ 5x\equiv 4 \pmod 6. \end{cases}$

237. Решить системы сравнений:

1) $\begin{cases} 17x\equiv 7 \pmod 2, \\ 2x\equiv 1 \pmod 3, \\ 2x\equiv 2 \pmod 5; \end{cases}$ 2) $\begin{cases} x\equiv 2 \pmod 3, \\ x\equiv 3 \pmod 2, \\ x\equiv -1 \pmod 6; \end{cases}$

3) $\begin{cases} 3x\equiv 5 \pmod 7, \\ 2x\equiv 3 \pmod 5, \\ 3x\equiv 3 \pmod 9; \end{cases}$ 4) $\begin{cases} 5x\equiv 200 \pmod{251}, \\ 11x\equiv 192 \pmod{401}, \\ 3x\equiv -151 \pmod{907}. \end{cases}$

238. Найти все натуральные числа, дающие в остатке 1 при делении на 2, на 3, на 4 и делящиеся на 5 без остатка.

239. Найти двузначное число, сравнимое с 2 по модулям 3 и 7, и с -2 по модулю 11.

240. Найти все целые числа, которые при делении на 2, на 3, на 4, на 5, на 6 и на 7 дают соответственно остатки 1, 2, 3, 4, 5 и 0.

241. Между 200 и 500 найти все целые числа, которые при делении на 4, 5 и 7 дают соответственно остатки 3, 4 и 5.

242. Найти целые точки прямых $4x-7y=9$, $2x+9y=15$ и $5x-13y=12$, лежащие на одном перпендикуляре к оси абсцисс.

243. Решить системы сравнений:

1) $\begin{cases} x\equiv a \pmod 6, \\ x\equiv 1 \pmod 8; \end{cases}$ 2) $\begin{cases} x\equiv 2 \pmod 6, \\ x\equiv a \pmod 8; \end{cases}$ 3) $\begin{cases} x\equiv 5 \pmod{18}, \\ x\equiv 8 \pmod{21}, \\ x\equiv a \pmod{35}; \end{cases}$

4) $\begin{cases} x\equiv a \pmod 7, \\ x\equiv b \pmod 5, \\ x\equiv c \pmod 3; \end{cases}$ 5) $\begin{cases} x\equiv 2 \pmod 4, \\ x\equiv -1 \pmod 3, \\ x\equiv 2 \pmod m, \text{ где } (m, 3) = \\ =(m, 4)=1. \end{cases}$

244. Найти значения a, при которых имеют решение системы:

1) $\begin{cases} x\equiv a \pmod 6, \\ x\equiv 1 \pmod{10}, \\ x\equiv 2 \pmod{21}, \\ x\equiv 3 \pmod{11}; \end{cases}$ 2) $\begin{cases} 2x\equiv a \pmod 4, \\ 3x\equiv 4 \pmod{10}. \end{cases}$

245. Найти хотя бы одно значение m, при котором не имеет решения система

$$\begin{cases} x \equiv 3 \pmod 6, \\ x \equiv 7 \pmod m. \end{cases}$$

246. Найти условия, которым должны удовлетворять модули m_1 и m_2, чтобы имела решение система

$$\begin{cases} x \equiv 3 \pmod 4, \\ x \equiv 4 \pmod{m_1}, \\ x \equiv 6 \pmod{m_2}. \end{cases}$$

247. Решить следующие сравнения сведением их к системам по попарно взаимно простым модулям:
1) $13x \equiv 32 \pmod{28}$; 2) $245x \equiv 405 \pmod{475}$; 3) $78x \equiv 49 \pmod{77}$; 4) $56x \equiv 81 \pmod{45}$.

248. Доказать, что система

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \end{cases}$$

где $(m_1, m_2) = 1$, имеет решение вида $x \equiv m_2 a_1 x_1 + m_1 a_2 x_2 \pmod{m_1 m_2}$, где x_1 и x_2 — значения неизвестного, удовлетворяющие соответственно сравнениям $m_2 x \equiv 1 \pmod{m_1}$ и $m_1 x \equiv 1 \pmod{m_2}$.

249. Применить теорему предыдущей задачи к решению систем:

1) $\begin{cases} x \equiv 3 \pmod 6, \\ x \equiv 2 \pmod 5; \end{cases}$ 2) $\begin{cases} x \equiv -1 \pmod{10}, \\ x \equiv 3 \pmod{99}. \end{cases}$

250. Следующие сравнения решить сведением их к системам сравнений по попарно взаимно простым модулям:
1) $x^3 + 2x + 3 \equiv 0 \pmod{15}$; 2) $x^2 \equiv -1 \pmod{20}$; 3) $x^2 \equiv -1 \pmod{85}$.

251. Решить системы сравнений:

1) $\begin{cases} x^2 + x \equiv 0 \pmod 2, \\ x^3 \equiv 2 \pmod 5; \end{cases}$ 2) $\begin{cases} x^3 + 3x^2 + 2x \equiv 0 \pmod 3, \\ x^2 - x \equiv 0 \pmod 2. \end{cases}$

252. Найти натуральные числа, удовлетворяющие условиям: 1) при делении на 7 они дают остаток 3; 2) их квадраты при делении на 7^2 дают остаток 44; 3) их кубы при делении на 7^3 дают остаток 111.

253. Найти целые числа, дающие при делении на нечетное натуральное число $m > 1$ остаток 1, такие, чтобы их квадраты при делении на m^2 давали остаток $m+1$.

254. Найти целые числа, удовлетворяющие условиям: 1) при делении на нечетный и отличный от 1 модуль m они дают остаток $m-1$; 2) их квадраты при делении на m^2 дают остаток 1.

255. Через какие целые точки проходят линии:

1) $15y=2x^3-5x^2+4x+11$, где $-2<x<8$;

2) $14y=3x^3-4x^2+11x+4$, где $-7<x<7$?

256. Решить сравнения с двумя неизвестными:

1) $x+2y\equiv 1 \pmod 3$; 2) $2x-3y\equiv 4 \pmod 5$;

3) $2x-y\equiv 1 \pmod 4$; 4) $3x+2y\equiv 5 \pmod 6$.

Обратить внимание на число решений каждого из этих сравнений. Решением сравнения $ax+by\equiv c \pmod m$ называется совокупность классов значений неизвестных, удовлетворяющих данному сравнению:

$$\left.\begin{matrix} x\equiv x_0 \\ y\equiv y_0 \end{matrix}\right\} \pmod m.$$

257. Доказать, что сравнение $ax+by\equiv c \pmod m$, где $(a, m)=1$, имеет m решений.

258. Сколько решений имеет сравнение $ax+by\equiv c \pmod m$, где $(a, b, m)=1$?

259. Решить сравнения: 1) $2x-6y\equiv 5 \pmod{15}$; 2) $3x+6y\equiv 2 \pmod 4$.

260. Сколько решений может иметь сравнение $ax+by\equiv c \pmod m$, где $(a, b, m)=d>1$?

261. Решить сравнения: 1) $3x+3y\equiv 3 \pmod 6$; 2) $2x-4y\equiv 6 \pmod 8$; 3) $4x+6y\equiv 10 \pmod{12}$; 4) $10x+5y\equiv 5 \pmod{35}$.

262. Решить системы сравнений:

1) $\begin{cases} x+3y\equiv 5 \\ 4x\equiv 5 \end{cases} \pmod 7$; 2) $\begin{cases} 9y\equiv 15 \\ 7x-3y\equiv 1 \end{cases} \pmod{12}$;

3) $\begin{cases} x\equiv 2 \\ x-2y\equiv 1 \end{cases} \pmod 4$; 4) $\begin{cases} 9y\equiv 15 \\ 3x-7y\equiv 1 \end{cases} \pmod{12}$;

5) $\begin{cases} 3x-5y\equiv 1 \\ 9y\equiv 15 \end{cases} \pmod{12}$.

263. Какое наибольшее число решений может иметь система

$$\begin{cases} ax\equiv b \\ a_1x+b_1y\equiv c \end{cases} \pmod m?$$

264. Решить системы сравнений:

1) $\begin{cases} x+2y\equiv 3 \\ 4x+y\equiv 2 \end{cases} \pmod 5$; 2) $\begin{cases} x+2y\equiv 0 \\ 3x+2y\equiv 2 \end{cases} \pmod 5$;

3) $\begin{cases} 3x+4y\equiv 29 \\ 2x-9y\equiv -84 \end{cases} \pmod{143}$; 4) $\begin{cases} x+2y\equiv 4 \\ 3x+y\equiv 2 \end{cases} \pmod 5$.

265. Решить системы сравнений:

1) $\begin{cases} x+5y\equiv 5 \\ 5x+3y\equiv 1 \end{cases} \pmod 6$; 2) $\begin{cases} 5x-y\equiv 3 \\ 2x+2y\equiv -1 \end{cases} \pmod 6$;

3) $\begin{cases} x-y\equiv 2 \\ 4x+2y\equiv 2 \end{cases} \pmod 6$; 4) $\begin{cases} 4x-y\equiv 2 \\ 2x+2y\equiv 0 \end{cases} \pmod 6$.

266. Доказать, что система

$$\begin{cases} a_1x+b_1y\equiv c_1 \\ a_2x+b_2y\equiv c_2 \end{cases} \pmod m, \tag{1}$$

где $(D, m)=1$ и $D=\begin{vmatrix} a_1 b_1 \\ a_2 b_2 \end{vmatrix}$, имеет единственное решение.

267. Найти условие, при котором система (1), где $(D, m)=d>1$, не имеет решений. Проверить найденное условие на системе

$$\begin{cases} 3x-2y\equiv 5 \\ 5x+2y\equiv 1 \end{cases} \pmod{20}.$$

268. Решить системы сравнений:

1) $\begin{cases} 2x+3y\equiv 1 \\ 3x-4y\equiv 3 \end{cases} \pmod 6$; 2) $\begin{cases} 4x+2y\equiv 3 \\ 3x+3y\equiv 2 \end{cases} \pmod 6$.

269. Доказать: множество решений системы (1), где

$$\begin{vmatrix} a_1 b_1 \\ a_2 b_2 \end{vmatrix} \equiv \begin{vmatrix} c_1 b_1 \\ c_2 b_2 \end{vmatrix} \equiv \begin{vmatrix} a_1 c_1 \\ a_2 c_2 \end{vmatrix} \equiv 0 \pmod m \text{ и } (a_1, m)=1,$$

совпадает с множеством решений первого сравнения.

270. Применить теорему предыдущей задачи к решению систем:

1) $\begin{cases} 3x+5y\equiv 2 \\ 6x+2y\equiv 4 \end{cases} \pmod 8$; 2) $\begin{cases} x+2y\equiv 2 \\ 2x+y\equiv 1 \end{cases} \pmod 3$.

271. Решить системы сравнений:

1) $\begin{cases} 3x+9y\equiv -3 \\ 2x+2y\equiv 10 \end{cases} \pmod{12}$; 2) $\begin{cases} 4x+2y\equiv 4 \\ 3x+3y\equiv 3 \end{cases} \pmod 6$;

3) $\begin{cases} 3x-2y\equiv 5 \\ 5x+2y\equiv 1 \end{cases} \pmod{10}$; 4) $\begin{cases} 3x-2y\equiv 5 \\ 5x+2y\equiv 1 \end{cases} \pmod{14}$.

272. Решить системы сравнений:

1) $\begin{cases} x+y\equiv 1 \pmod 4, \\ 5x+2y\equiv 8 \pmod{12}; \end{cases}$ 2) $\begin{cases} 2x-y\equiv 3 \pmod 4, \\ x+2y\equiv 2 \pmod 3; \end{cases}$

3) $\begin{cases} x+y\equiv 1 \pmod 4, \\ 2x-y\equiv 1 \pmod 6; \end{cases}$ 4) $\begin{cases} x-y\equiv 1 \pmod 3, \\ x+y\equiv 1 \pmod 2; \end{cases}$

5) $\begin{cases} x-y\equiv 2 \pmod 3, \\ 5x+3y\equiv 1 \pmod 6. \end{cases}$

273. Доказать, что система

$$\begin{cases} 5x+y\equiv 3 \pmod{33}, \\ x+2y\equiv 1 \pmod{21} \end{cases}$$

не имеет решений.

274. Найти критерий разрешимости системы

$$\begin{cases} a_1x+b_1y\equiv c_1 \pmod{m_1}, \\ a_2x+b_2y\equiv c_2 \pmod{m_2}. \end{cases}$$

Применить найденный критерий к системе предыдущей задачи.

275. Найти все числа вида $\overline{xy2}$, делящиеся на 28.

276. Найти все числа вида $\overline{xy9z}$, делящиеся на 132.

277. Найти все пары чисел вида $\overline{1xy2}$ и $\overline{x12y}$, такие, чтобы оба числа делились на 7.

278. Доказать, что не существует чисел вида $\overline{xy2}$ и $\overline{2xy}$, которые оба делятся на 7.

279. Решить в целых числах системы уравнений:

1) $\begin{cases} x+2y+5z=1, \\ 3x+y+5z=3; \end{cases}$ 2) $\begin{cases} x-y-3z=1, \\ x+y-2z=1. \end{cases}$

280. Найти все целые числа x и y, такие, чтобы числа вида $\frac{3x-y+1}{7}$ и $\frac{2x+3y-1}{7}$ также были целыми.

§ 11. Квадратичные вычеты

Всякое сравнение второй степени с одним неизвестным по нечетному простому модулю, т. е. сравнение вида $ax^2+bx+c\equiv 0 \pmod p$, где $a\not\equiv 0 \pmod p$, может быть приведено к двучленному сравнению вида $y^2\equiv d \pmod p$, где $y=2ax+b$ и $d=b^2-4ac$.

Двучленное сравнение вида $x^2\equiv a \pmod p$, где $a\not\equiv 0 \pmod p$ и $p>2$, либо не имеет решений, либо имеет два решения. В первом случае число a называют квадратичным невычетом, а во втором — квадратичным вычетом по модулю p.

Чтобы число a было квадратичным вычетом по модулю p, необходимо и достаточно, чтобы $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ (критерий Эйлера).

Число a, удовлетворяющее условию $a \not\equiv 0$ (mod $p > 2$), удовлетворяет одному и только одному из сравнений:

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

(во втором случае число a является квадратичным невычетом по модулю p). Эти сравнения объединяются сравнением

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

где $\left(\frac{a}{p}\right)$ — символ Лежандра (числа a по модулю p), которому приписывается значение 1, если a — квадратичный вычет, и -1, если a — квадратичный невычет по модулю p.

Основные свойства символа Лежандра:

1) чтобы $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, необходимо и достаточно, чтобы $a \equiv b \pmod p$;

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

3) $\left(\frac{a_1 a_2 \ldots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \ldots \left(\frac{a_n}{p}\right)$;

4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

5) если p и q — различные нечетные простые числа, то $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}\left(\frac{q}{p}\right)$ (закон квадратичной взаимности).

281. Решить сравнения, предварительно приведя их к двучленному: 1) $2x^2+4x-1 \equiv 0 \pmod 5$; 2) $3x^2+2x \equiv 1 \pmod 7$; 3) $2x^2-2x-1 \equiv 0 \pmod 7$; 4) $3x^2-x \equiv 0 \pmod 5$.

282. Доказать: сравнение $ax^2+bx+c \equiv 0$ (mod $p > 2$), где $a \not\equiv 0 \pmod p$ и $b^2 \not\equiv 4ac \pmod p$, разрешимо тогда и только тогда, когда

$$(b^2-4ac)^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

283. Доказать, что сравнение $ax^2+bx+c \equiv 0 \pmod{p > 2}$, где $a \not\equiv 0 \pmod p$ и $b^2 \equiv 4ac \pmod p$, имеет в точности одно решение.

284. При каких натуральных значениях x следующие функции принимают целочисленные значения:

1) $\frac{x^2+2x+7}{55}$; 2) $\frac{x^2+3x+1}{25}$; 3) $\frac{x^2+3x+5}{15}$?

285. Решить сравнение $x^2 \equiv a \pmod p$, если: 1) $a \equiv 0 \pmod p$; 2) $p=2$.

286. Доказать, что по данному модулю общее число классов квадратичных вычетов и невычетов четное.

287. Доказать, что число классов квадратичных вычетов всегда равно числу классов квадратичных невычетов (по данному модулю).

288. Доказать, что при $a^{\frac{p-1}{2}} \equiv 1 \pmod{p > 2}$ сравнение имеет два решения.

289. Найти значения параметра a, при которых сравнение $ax \equiv 1 \pmod{p > 2}$, где $(a, p)=1$, имеет решение $x \equiv a \pmod p$.

290. При помощи критерия Эйлера установить, какие из следующих сравнений разрешимы, и найти соответствующие решения: 1) $x^2 \equiv -3 \pmod 7$; 2) $x^2 \equiv 3 \pmod{11}$; 3) $x^2 \equiv 6 \pmod 7$; 4) $x^2 \equiv 340 \pmod{13}$.

291. Доказать, что произведение квадратичных вычетов по данному модулю есть квадратичный вычет по этому модулю (в частности, натуральная степень квадратичного вычета есть квадратичный вычет по данному модулю), произведение квадратичных невычетов есть квадратичный вычет по данному модулю, если число сомножителей четное (в частности, четная натуральная степень квадратичного невычета есть квадратичный вычет по данному модулю), но произведение квадратичного вычета и невычета есть квадратичный невычет по данному модулю.

292. Найти все классы квадратичных вычетов по модулям 5, 7, 11 и 13.

293. Доказать, что числа $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$ образуют систему представителей всех классов квадратичных вычетов по модулю $p>2$.

294. Найти значения a, при которых имеют решения сравнения:
1) $x^2 \equiv a \pmod 3$; 2) $x^2 \equiv a \pmod 5$; 3) $x^2 \equiv a \pmod 7$; 4) $x^2 \equiv a \pmod{11}$.

295. Доказать, что сравнение $x^2+1 \equiv 0 \pmod p$ имеет решения тогда и только тогда, когда $p=4n+1$ $(n=1, 2, 3, \ldots)$.

296. Доказать, что каноническое разложение чисел вида a^2+b^2, где $(a, b)=1$, содержит простые числа вида $4n+1$ $(n=1, 2, 3, \ldots)$, и только такие простые числа.

297. Доказать, что произведение двух последовательных целых чисел не может быть сравнимо с 1 по модулю 13.

298. Найти все значения a, при которых сравнение $x(x+1) \equiv a \pmod{13}$ имеет решения.

299. При помощи теоремы задачи 295 доказать, что существует бесконечное множество простых чисел вида $4n+1$ $(n=1, 2, 3, \ldots)$.

300. Решить в целых числах уравнения (найти целые точки, через которые проходят следующие кривые): 1) $4x^2-5y=6$; 2) $11y=5x^2-7$; 3) $x^2-10x-11y+5=0$; 4) $13y=x^2-21x+110$; 5) $15x^2-7y^2=9$.

301. Доказать, что сравнение $x^2 \equiv a \pmod{p=4n+3}$, где $\left(\frac{a}{p}\right)=1$, имеет решения: $x \equiv \pm a^{n+1} \pmod p$.

302. По модулю $p=4n+3$ одно из чисел a и $-a$ является квадратичным вычетом, другое — невычетом; по модулю $p=4n+1$ числа a и $-a$ либо оба квадратичные вычеты, либо оба квадратичные невычеты. Доказать.

303. Зная, что a — квадратичный вычет по модулю $p=8n+5$, решить сравнение $x^2 \equiv a \pmod p$.

304. Найти модули, по которым следующие числа являются квадратичными вычетами (невычетами): 1) $a=5$; 2) $a=-3$; 3) $a=3$; 4) $a=2$; 5) $a=-7$.

305. Найти все нечетные простые модули, по которым имеют решения сравнения: 1) $x(x+1) \equiv 1 \pmod p$; 2) $x(x-1) \equiv 2 \pmod p$; 3) $x(x-1) \equiv 3 \pmod p$.

306. При помощи символа Лежандра доказать, что независимо от модуля $p>2$ разрешимы следующие сравнения: 1) $(x^2-13)(x^2-17)(x^2-221) \equiv 0 \pmod p$;
2) $(x^2-3)(x^2-5)(x^2-7)(x^2-11)(x^2-1155) \equiv 0 \pmod p$.

307. Доказать, что: 1) $\left(\frac{a^n}{p}\right)=\left(\frac{a}{p}\right)^n$; 2) $\left(\frac{-q}{p}\right)=(-1)^{\frac{q+1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{q}\right)$, где q и p — различные нечетные простые числа.

308. Вычислить символы Лежандра: 1) $\left(\frac{13}{7}\right)$; 2) $\left(\frac{22}{13}\right)$; 3) $\left(\frac{426}{491}\right)$; 4) $\left(\frac{37}{67}\right)$.

309. Найти значение суммы $\sum_{x=2}^{p-1}\left(\frac{x}{p}\right)$.

310. При помощи символа Лежандра установить, какие из следующих сравнений разрешимы: 1) $x^2\equiv5 \pmod{19}$; 2) $x^2\equiv5 \pmod{29}$; 3) $x^2\equiv2 \pmod{97}$; 4) $x^2\equiv241 \pmod{587}$; 5) $x^2\equiv151 \pmod{587}$.

311. Не решая сравнений $x^2\equiv13 \pmod{41}$ и $x^2\equiv41 \pmod{13}$, установить, что они оба либо имеют решения, либо не имеют решений. Какая именно из этих возможностей имеет место?

312. Символ Якоби $\left(\frac{a}{m}\right)$ для нечетного $m=p_1p_2\ldots p_k$, где p_i — числа простые, среди которых могут быть равные, и $(a, m)=1$, определяется равенством $\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_k}\right)$, где $\left(\frac{a}{p_i}\right)$ — символы Лежандра.

Доказать, что символ Якоби обладает всеми основными свойствами символа Лежандра.

313. Применить символ Якоби к исследованию сравнений: 1) $x^2\equiv903 \pmod{2111}$; 2) $x^2\equiv219 \pmod{383}$; 3) $x^2\equiv7 \pmod{1964}$.

314. Доказать теорему: сравнение $x^2\equiv a \pmod{p^\alpha}$, где a не делится на нечетное простое число p, имеет решение тогда и только тогда, когда $\left(\frac{a}{p}\right)=1$.

315. При помощи теоремы предыдущей задачи установить, какие из следующих сравнений разрешимы, и найти соответствующие решения: 1) $x^2\equiv7 \pmod{27}$; 2) $x^2\equiv59 \pmod{125}$.

316. Решить уравнение $\left(\frac{a}{15}\right)=1$, где $\left(\frac{a}{15}\right)$ — символ Якоби.

317. Доказать, что среди дискриминантов квадратных уравнений с одним неизвестным и целыми коэффициентами не может встретиться чисел вида $4n+2$ или $4n+3$.

318. Доказать, что сравнение $x^2 \equiv -7 \pmod{p^\alpha}$, где p — нечетное простое число вида $7n+1$, разрешимо при любом натуральном значении α.

319. Доказать, что сравнение $x^2 \equiv -11 \pmod{4p}$, где p — нечетное простое число вида $11n+2$, неразрешимо.

320. Может ли сумма $1+2+3+ \ldots +n$ при каком-нибудь натуральном значении n оканчиваться цифрой 7?

§ 12. Степенные вычеты

По теореме Эйлера сравнению $a^x \equiv 1 \pmod m$, где $(a, m)=1$, удовлетворяет $x=\varphi(m)$. Наименьшее натуральное значение x, удовлетворяющее данному сравнению, называется показателем, которому принадлежит число a по модулю m, и обозначается символом $P_m(a)$. Основные свойства показателей:

1) Чтобы $a^x \equiv 1 \pmod m$, $(a, m)=1$, необходимо и достаточно, чтобы $x \equiv 0 \pmod{P_m(a)}$ или $x=P_m(a)\cdot n$, $n=1, 2, \ldots$ (формула общего решения данного сравнения); таким образом, $\varphi(m) \vdots P_m(a)$.

2) Если $a \equiv b \pmod m$, то $P_m(a)=P_m(b)$.

3) Числа $a, a^2, a^3, \ldots, a^{P_m(a)}$ попарно несравнимы по модулю m.

4) Чтобы $P_m(a^x)=P_m(a)$, где $x=1, 2, \ldots, P_m(a)$, необходимо и достаточно, чтобы $(x, P_m(a))=1$.

Если $P_m(a)=\varphi(m)$, то число a называется первообразным корнем модуля m.

Первообразные корни имеют лишь следующие модули: 2, 4, p^α и $2p^\alpha$, где p — нечетное простое число. Если модуль m имеет первообразные корни, то число их классов равно $\varphi(\varphi(m))$.

Чтобы существовало значение x, удовлетворяющее сравнению $a^x \equiv b \pmod m$, где $(a, m)=1$, необходимо, чтобы $(b, m)=1$. Если при этом $P_m(a)=\varphi(m)$, то непременно существуют значения x, удовлетворяющие данному сравнению, составляющие один класс по модулю $P_m(a)$: $x \equiv x_0 \pmod{P_m(a)}$.

Значения x, удовлетворяющие данному сравнению, называются индексами числа b по основанию a и модулю m:

$$x=\mathrm{ind}_a b \pmod m.$$

Определение индекса может быть записано в виде

$$a^{\mathrm{ind}_a b} \equiv b \pmod m.$$

Пользуясь этим определением, можно составить таблицу индексов по данным основанию и модулю.

Основные свойства индексов:

1) Чтобы $b_1 \equiv b_2 \pmod{m}$, необходимо и достаточно, чтобы $\operatorname{ind}_a b_1 \equiv \operatorname{ind}_a b_2 \pmod{P_m(a)}$; переход от первого сравнения ко второму называется индексированием; переход от второго к первому — потенцированием.

2) $\operatorname{ind}_a 1 \equiv 0 \pmod{P_m(a)}$.

3) $\operatorname{ind}_a a \equiv 1 \pmod{P_m(a)}$.

4) $\operatorname{ind}_a (b_1 b_2 \ldots b_n) \equiv \operatorname{ind}_a b_1 + \operatorname{ind}_a b_2 + \ldots + \operatorname{ind}_a b_n \pmod{P_m(a)}$, в частности, $\operatorname{ind}_a b^n \equiv n \operatorname{ind}_a b \pmod{P_m(a)}$.

Часто применяются системы индексов по нечетному простому модулю и одному из его первообразных корней как основанию.

321. Найти $P_m(m-1)$.

322. Найти все классы, принадлежащие показателю 2 по модулю 8.

323. Найти показатель, которому принадлежит класс $x \equiv 2 \pmod{11}$.

324. Найти все возможные показатели по модулю 9.

325. Найти все натуральные значения x, удовлетворяющие сравнениям: 1) $5^x \equiv 1 \pmod 8$; 2) $4^x \equiv 1 \pmod 3$.

326. Доказать теорему: если $P_p(a) = 2\alpha$, то $a^\alpha + 1 \equiv 0 \pmod p$.

327. Доказать, что числа $2, 2^2, 2^3, \ldots, 2^{10}$ образуют приведенную систему вычетов по модулю 11.

328. Доказать, что простые делители числа $2^{2^n}+1$ ($n = 1, 2, \ldots$) имеют вид $k \cdot 2^{n+1}+1$ (например, простой делитель числа $2^{2^5}+1$ имеет вид $64k+1$; так, при $k=10$ имеем делитель 641).

329. Доказать, что $\varphi(a^m-1) \equiv 0 \pmod m$, где $a > 1$.

330. Решить сравнения: 1) $5^x \equiv 1 \pmod 9$; 2) $2^x \equiv 1 \pmod{25}$; 3) $6^x \equiv 1 \pmod{49}$; 4) $2^x \equiv 1 \pmod{49}$.

331. Найти число классов и сами классы первообразных корней модуля 7.

332. Найти все классы первообразных корней модуля 6.

333. Доказать, что модуль 8 не имеет первообразных корней.

334. Найти все значения b, при которых разрешимы сравнения: 1) $5^x \equiv b \pmod 9$; 2) $4^x \equiv b \pmod 9$.

335. Определить число классов значений b, которым соответствует сравнение $a^x \equiv b \pmod m$, где $(a, m) = 1$, не имеющее решений.

336. Найти все возможные основания индексов по модулю 11 и составить таблицу индексов при наименьшем из найденных оснований.

337. При помощи индексов найти показатель, которому принадлежит 6 по модулю 23.

338. При помощи индексов доказать, что 2 есть первообразный корень модуля 37.

339. Доказать, что $P_p(a) = p-1$ тогда и только тогда, когда $(\operatorname{ind} a, p-1) = 1$.

340. Опираясь на теорему предыдущей задачи, найти все классы первообразных корней модуля 13.

341. При помощи индексов решить сравнения: 1) $8x \equiv -11 \pmod{37}$; 2) $x^2 \equiv 3 \pmod{11}$; 3) $x^5 \equiv 14 \pmod{41}$; 4) $13x^{21} \equiv 5 \pmod{31}$; 5) $40x^{10} \equiv 3 \pmod{17}$; 6) $x^2 \equiv 89 \pmod{97}$.

342. При каких целых значениях a:
1) $3a^2-5 \,\vdots\, 7$; 2) $7a^2+13 \,\vdots\, 23$; 3) $13a^2-11 \,\vdots\, 29$?

343. При помощи индексов решить сравнения:
1) $2^x \equiv 7 \pmod{67}$; 2) $13^x \equiv 12 \pmod{47}$; 3) $21^{3x} \equiv 21^5 \pmod{29}$.

344. Доказать, что индекс -1 по нечетному модулю p всегда равен $\frac{p-1}{2}$.

345. Обобщить критерий Эйлера на случай сравнения $x^n \equiv a \pmod p$, где $a \not\equiv 0 \pmod{p>2}$.

346. При помощи обобщения критерия Эйлера (см. предыдущую задачу) установить, какие из следующих сравнений разрешимы, и найти соответствующие решения: 1) $x^5 \equiv 20 \pmod 7$; 2) $x^6 \equiv 9 \pmod{11}$; 3) $3x^8 \equiv 5 \pmod{13}$.

347. Доказать, что число a, для которого $a \not\equiv 0 \pmod{p>2}$, является квадратичным вычетом по модулю p тогда и только тогда, когда $\operatorname{ind} a \equiv 0 \pmod 2$. При помощи таблицы индексов найти все классы квадратичных вычетов по модулю 23.

348. Вывести формулу перехода от одной системы индексов к другой по данному модулю.

349. Доказать, что первообразный корень модуля $p>2$ является квадратичным вычетом по этому модулю.

350. Доказать, что среди первообразных корней простого модуля не может быть квадратов.

351. Доказать, что a^{2n+1} ($n=0, 1, 2, \ldots$) является квадратичным вычетом по модулю $p>2$, если a — первообразный корень модуля p.

352. Доказать, что произведение двух первообразных корней модуля $p>2$ не может быть первообразным корнем этого модуля.

353. Доказать, что модуль 2^n ($n=3, 4, 5, \ldots$) не имеет первообразных корней.

§ 13. Арифметические приложения сравнений

Задача вычисления остатка r от деления данного числа a на модуль m (его можно обозначить символом $r(a, m)$) по существу уже встречалась в предыдущих параграфах. Она сводится к получению сравнения $a \equiv \equiv r \pmod m$, $0 \leqslant r < m$. Особенно эффективно применение сравнений к вычислению остатков от деления степеней и произведений; это видно из следующих примеров:

1) $1967^{1968} \equiv 9^{1968} \pmod{11}$; так как $9^{10} \equiv 1 \pmod{11}$, то $9^{1968} \equiv 9^8 \equiv 81^4 \equiv 4^4 \equiv 16^2 \equiv 25 \equiv 3 \pmod{11}$. Таким образом, $r(1967^{1968}, 11)=3$;

2) $8! = (2.6)\,(3.4)\,(5.7).8 = 1.1.2.8 \equiv 5 \pmod{11}$ и $r(8!, 11)=5$.

В ряде случаев могут быть использованы индексы:

1) индексируя сравнение $r \equiv 9^{1968} \pmod{11}$, получаем $\operatorname{ind} r \equiv 1968.6 \equiv 8.6 \equiv 8 \pmod{10}$, откуда $r=3$ (см. таблицу);

2) индексируя сравнение $r \equiv 8! \pmod{11}$, получаем $\operatorname{ind} r \equiv 1+8+2+4+9+7+3=34 \equiv 4 \pmod{10}$, откуда $r=5$.

Весьма эффективным является применение сравнений к установлению признаков делимости. Так, чтобы установить признак делимости на 101, достаточно заметить, что $100 \equiv -1 \pmod{101}$; в соответствии с этим имеем:

$$\overline{a_n, \ldots, a_1a_0} = \overline{a_1a_0} + 100\overline{a_3a_2} + 100^2\overline{a_5a_4} + \ldots \equiv$$

$$\equiv \overline{a_1a_0} - \overline{a_3a_2} + \overline{a_5a_4} - \ldots \pmod{101}.$$

Таким образом, число делится на 101 тогда и только тогда, когда на 101 делится разность между суммой его граней, стоящих на нечетных местах, и суммой остальных граней (число разбивается на грани, как при извлечении квадратного корня). Например, $1083831 \vdots 101$, так как $(31+8)-(38+1)=0 \vdots 101$, но 3406326 не $\vdots 101$, так как $(26+40)-(63+3)=2$ не $\vdots 101$.

Понятие показателя находит применение при определении длины наименьшего периода бесконечной десятичной дроби, заданной обыкновенной дробью. Если знаменатель данной обыкновенной дроби (несократимой) есть $2^{\alpha} \cdot 5^{\beta} m$, где $(m, 10)=1$, то длина наименьшего периода соответствующей бесконечной десятичной дроби равна показателю, которому принадлежит 10 по модулю m, т. е. равна $P_m(10)$.

Теория сравнений дает способ проверки арифметических действий «с помощью девятки», основанный на теореме: если s, s_1 и s_2 — суммы цифр соответственно чисел m, m_1 и m_2, то из $m=m_1 \pm m_2$ или $m=m_1 m_2$ следует соответственно $s=s_1 \pm s_2 \pmod 9$ или $s=s_1 s_2 \pmod 9$.

Эта теорема дает возможность обнаружить ошибку в арифметических действиях, если таковая есть. Следует иметь в виду, что обратная теорема не верна, например, $8.2 \equiv 16 \pmod 9$, но $71.11 \not\equiv 871$.

354. Найти остаток от деления: 1) 2^{64} на 360; 2) 1532^5-1 на 9; 3) $(1237^{156}+34)^{28}$ на 111; 4) $8!$ на 11; 5) a на 13, если $a^x \equiv 2 \pmod{13}$ и $a^{x+1} \equiv 6 \pmod{13}$.

355. Применить теорему Эйлера при нахождении остатка от деления: 1) 174^{249} на 13; 2) 1863^5-5 на 10; 3) $2^{37 \cdot 73-1}$ на 37.73.

356. Найти последние две цифры чисел: 1) 203^{20}; 2) 243^{402}; 3) 1812.1941.1965; 4) $(116+17^{17})^{21}$.

357. Доказать, что: 1) $(2^{32}+1) \vdots 641$; 2) $(222^{555}+555^{222}) \vdots 7$; 3) $(220^{119^{69}}+69^{220^{119}}+119^{69^{220}}) \vdots 102$; 4) $(6^{2n+1}+5^{n+2}) \vdots 31$.

358. Найти остаток от деления $4^{\varphi(m)-1}$ на нечетное число $m>1$.

359. При помощи индексов найти остаток от деления: 1) 10^{10} на 67; 2) 178^{52} на 11; 3) 1967^{1968} на 11.

360. Применить общий признак делимости Паскаля, выражающийся сравнением $N=a_n \ldots a_1 a_0 \equiv a_n r_n + \ldots + a_1 r_1 + a_0 \pmod m$, где r_i — остатки от деления 10^i на m, к установлению признаков делимости: 1) на 6; 2) на 8; 3) на 12; 4) на 15; 18 и 45.

361. Вывести признак делимости на 11 на основании сравнения $10 \equiv -1 \pmod{11}$ и теоремы: по данному модулю сравнимым значениям аргумента соответствуют сравнимые значения полинома с целыми коэффициентами.

362. Вывести общий признак делимости на 7 и на 13 на основании сравнения $1000 \equiv -1 \pmod{7;\ 13}$.

363. Вывести общий признак делимости на 27 и на 37, исходя из сравнения $10^3 \equiv 1 \pmod{27;\ 37}$.

364. Доказать, что $N = \overline{a_n \ldots a_1 a_0} \equiv 0 \pmod{m}$, где $(m, 10) = 1$, тогда и только тогда, когда $\overline{a_n \ldots a_2 a_1} + a_0 x \equiv 0 \pmod{m}$, где x удовлетворяет сравнению $10x \equiv 1 \pmod{m}$.

365. Применить теорему предыдущей задачи к установлению делимости: 1) 185231 на 19; 2) 448721 на 13; 3) 192843 на 7; 4) 67749 на 11.

366. Доказать, что $N = \overline{a_n \ldots a_1 a_0} = 10 \cdot A + a_0 \equiv \equiv 0 \pmod{m}$, где $(m, 10) = 1$, тогда и только тогда, когда $q + r a_0 \equiv 0 \pmod{m}$, где q и r — частное и остаток от деления A на число $x > 0$, удовлетворяющее сравнению $10x \equiv 1 \pmod{m}$. При $x < 0$ критерий делимости выражается сравнением $-q + r a_0 \equiv 0 \pmod{m}$.

367. Найти все числа вида $\overline{13xy45z}$, делящиеся на 792.

368. Найти все системы счисления, в которых число делится на 2 тогда и только тогда, когда сумма его цифр делится на 2. Решить задачу, заменив модуль 2 произвольным натуральным числом $m > 1$.

369. Найти наименьшее основание системы счисления, в которой имеют место признаки делимости:

1) число делится на 5 тогда и только тогда, когда сумма его цифр делится на 5;

2) число делится на 7 тогда и только тогда, когда на 7 делится число, составленное двумя последними его цифрами.

370. Не представляя следующих обыкновенных дробей в виде бесконечных десятичных, найти длину периода: 1) $\frac{4}{21}$; 2) $\frac{9}{91}$; 3) $\frac{1}{43}$; 4) $\frac{a}{97}$, где $(a, 97) = 1$.

371. Найти длину периода бесконечных десятичных дробей, заданных следующими обыкновенными дробями: 1) $\frac{1}{14}$; 2) $\frac{7}{550}$.

372. Найти знаменатель обыкновенной дроби вида $\frac{1}{m}$, которая представляется чистой периодической десятичной дробью с двумя цифрами в периоде.

373. Найти длину периода бесконечных десятичных дробей, заданных следующими обыкновенными дробями: 1) $\frac{10}{17 \cdot 23}$; 2) $\frac{1}{53 \cdot 59}$.

374. Доказать, что обыкновенная дробь $\frac{1}{p_1 p_2}$, где p_1 и p_2 — простые числа, отличные от 2 и 5, представляется периодической бесконечной десятичной дробью с длиной периода $\left[\frac{p_1-1}{d_1}, \frac{p_2-1}{d_2}\right]$, где $d_1=(\text{ind } 10, \; p_1-1)$ и $d_2=$ $=(\text{ind } 10, \; p_2-1)$ (в первом случае ind 10 берется по модулю p_1, во втором — по модулю p_2).

375. При помощи теории сравнений показать ошибочность следующих записей: 1) $4237 \cdot 27925 = 118275855$; 2) $42981 : 8264 = 5201$; 3) $1965^2 = 3761225$.

376. Привести пример, когда условие $s(m_1) \cdot s(m_2) \equiv$ $\equiv s(m) \pmod 9$ выполняется, но $m_1 m_2 \neq m$.

377. Найти способ проверки «с помощью девятки» при извлечении корня любой степени.

Найденным способом показать ошибочность записи: $\sqrt[5]{371293} = 23$.

ГЛАВА 3

НЕПРЕРЫВНЫЕ ДРОБИ

§ 14. Основные понятия

Конечная непрерывная дробь

$$q_0+\cfrac{1}{q_1+\cfrac{}{q_2+\ldots\ldots\ldots\ldots \atop \ldots\ldots\ldots\ldots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}}=(q_0,\ q_1,\ldots,q_n),$$

где q_i — целые числа, из которых q_i $(i\geqslant 1)$ — натуральные, является символом рационального числа: каждое рациональное число разлагается в определенную конечную непрерывную дробь и каждая конечная непрерывная дробь свертывается в определенное рациональное число (при условии, что $q_n>1$).

Каждое иррациональное число разлагается в бесконечную непрерывную дробь $(q_0, q_1, q_2, \ldots)$, которая может быть периодической — чистой или смешанной (см. принятые обозначения). Отрезок $(q_0, q_1, q_2, \ldots, q_k)$ непрерывной дроби (конечной или бесконечной) называется подходящей дробью k-го порядка и обозначается $\frac{P_k}{Q_k}$. По определению

$$\frac{P_0}{Q_0}=(q_0)=\frac{q_0}{1} \text{ и } \frac{P_1}{Q_1}=(q_0,\ q_1)=q_0+\frac{1}{q_1}=\frac{q_0q_1+1}{q_1}.$$

Эти формулы называются начальными данными. При $k\geqslant 2$ имеет место рекуррентная формула:

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

С возрастанием порядка знаменатели подходящих дробей возрастают, начиная с Q_1 (числители также возрастают, начиная с P_0).

378. Разложить в непрерывную дробь: $\frac{127}{52}$, $\frac{24}{35}$ и 1,23.

379. Свернуть непрерывные дроби: (1,1, 2,1, 2,1,2); (0,1,2,3,4,5); (5,4,3,2,1); (a, a, a, a, a); (a, b, a, b, a).

380. Решить уравнения: 1) $(x, 2, 3, 4)=\frac{73}{30}$;
2) $7(xyz+x+z)=10(yz+1)$.

381. Разложить в непрерывную дробь $\sqrt{2}$, $\sqrt{7}$, $\frac{5+\sqrt{2}}{2}$.

382. Разложить в непрерывную дробь положительные корни трехчленов: $2x^2+2x-3$ и $4x^2-12x+7$.

383. Найти частное от деления непрерывной дроби $(2,2,2, \ldots, 2)$ на 2.

384. Доказать, что

$$\left(\frac{P_{n+2}}{P_n}\right)\left(1-\frac{P_{n-1}}{P_{n+1}}\right)=\left(\frac{Q_{n+2}}{Q_n}-1\right)\left(1-\frac{Q_{n-1}}{Q_{n+1}}\right).$$

385. Доказать, что $\frac{P_n}{P_{n-1}}=(a_n, \ldots, a_1, a_0)$ и $\frac{Q_n}{Q_{n-1}}=$ $=(a_n, \ldots, a_2, a_1)$, где P_i и Q_i — элементы подходящих дробей непрерывной дроби $(a_0, \ldots, a_{n-1}, a_n)$, $a\geqslant 1$ и $n\geqslant 1$.

386. Доказать несократимость дробей $\frac{P_n}{P_{n-1}}$ и $\frac{Q_n}{Q_{n-1}}$.

387. Доказать, что $(2,2,\ldots,2)=\frac{(1+\sqrt{2})^{n+1}-(1-\sqrt{2})^{n+1}}{(1+\sqrt{2})^n-(1-\sqrt{2})^n}$, где непрерывная дробь содержит n неполных частных.

§ 15. Сходимость бесконечной непрерывной дроби

Подходящие дроби обладают следующими основными свойствами:

1) $\frac{P_k}{Q_k}-\frac{P_{k-1}}{Q_{k-1}}=\frac{(-1)^{k-1}}{Q_k Q_{k-1}}$ или $P_kQ_{k-1}-Q_kP_{k-1}=(-1)^{k-1}$,

где $k=1, 2, \ldots$

Из начальных условий и этого свойства вытекает, что $(P_k, Q_k)=1$.

2) С возрастанием порядка подходящие дроби четного порядка возрастают, а нечетного убывают, причем каждая подходящая дробь четного порядка меньше любой подходящей дроби нечетного порядка.

3) $\alpha=(q_0, q_1, \ldots, q_k, \alpha_{k+1})=\dfrac{P_k\alpha_{k+1}+P_{k-1}}{Q_k\alpha_{k+1}+Q_{k-1}}$, где $k=1, 2, \ldots$ и $\alpha_{k+1}=(q_{k+1}, q_{k+2}, \ldots)$.

4) Каждая бесконечная непрерывная дробь $(q_0, q_1, q_2, \ldots)$ свертывается в иррациональное число α, такое, что

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

и

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

Подходящая дробь $\frac{P_k}{Q_k}$ является наилучшим рациональным приближением действительного числа α, т. е. никакая рациональная дробь $\frac{x}{y}$, у которой $y\leqslant Q_k$, не может быть ближе к α, чем $\frac{P_k}{Q_k}$. Дробь $\frac{P_k}{Q_k}$ является приближением α с точностью до $\frac{1}{Q_kQ_{k+1}}$. Чтобы с помощью подходящих дробей найти приближение α с заданной точностью ε, достаточно, чтобы $Q_k>\sqrt{\frac{1}{\varepsilon}}$; однако заданной мере точности может удовлетворять подходящая дробь меньшего порядка.

388. При помощи разложения в непрерывную дробь сократить: 1) $\frac{3587}{2743}$; 2) $\frac{1043}{3427}$; 3) $\frac{1491}{2247}$.

389. Доказать несократимость дроби вида $\frac{a^4+3a^2+1}{a^3+2a}$, где a — число натуральное.

390. Доказать, что для симметричной конечной непрерывной дроби $(q_n=q_0, q_{n-1}=q_1=\ldots)$ имеет место соотношение $P_{n-1}=Q_n$.

391. Доказать, что $Q_n\geqslant 2^{\frac{n-1}{2}}$ $(n\geqslant 2)$.

392. Применить соотношение $P_nQ_{n-1}-Q_nP_{n-1}=(-1)^{n-1}$ к решению сравнения $ax\equiv b \pmod m$, где $(a, m)=1$.

393. Решить найденным способом сравнения: 1) $95x\equiv 59 \pmod{308}$; 2) $91x\equiv 1 \pmod{132}$.

394. Применить соотношение $P_nQ_{n-1}-Q_nP_{n-1}=(-1)^{n-1}$ к решению в целых числах уравнения $ax+by=c$.

395. Решить найденным способом уравнения: 1) $70x+33y=1$; 2) $60x-91y=2$; 3) $571x+359y=-10$.

396. Следующие числа заменить подходящей дробью третьего порядка и оценить погрешность: 1) $\frac{587}{103}$; 2) 3,14159; 3) $\frac{-1+\sqrt{5}}{2}$; 4) $\frac{2-\sqrt{3}}{5}$.

397. При помощи зубчатой передачи, состоящей из двух шестерен, требуется установить между их осями отношение угловых скоростей вращения, близкое к 355:113, чтобы погрешность не превышала 0,002. Можно ли осуществить такую передачу при помощи меньшего числа зубцов, чем 355 и 113?

398. Число $\frac{1261}{881}$ заменить подходящей дробью с возможно меньшим знаменателем так, чтобы погрешность не превышала 0,0001.

399. Найти наилучшее приближение с точностью до 0,001: 1) $\sqrt{2}$; 2) $\sqrt{11}$.

400. Найти с точностью до 0,0001 наилучшие приближения корней следующих уравнений: 1) $x^2-5x+2=0$; 2) $4x^2+20x+23=0$.

401. Доказать, что $\left|\alpha-\frac{P_n}{Q_n}\right|>\frac{1}{Q_n(Q_n+Q_{n+1})}$, предварительно убедившись, что $\frac{P_n}{Q_n}$ и $\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}$ лежат по одну сторону от α.

402. Увеличивается или уменьшается подходящая дробь n-го порядка, если неполное частное q_n увеличить на несколько единиц?

403. Если число α имеет подходящую дробь порядка $n\geqslant 1$, то имеет место по крайней мере одно из неравенств:

$$\left|\alpha-\frac{P_n}{Q_n}\right|<\frac{1}{2Q_n^2}$$

или

$$\left|\alpha-\frac{P_{n-1}}{Q_{n-1}}\right|<\frac{1}{2Q_{n-1}^2}.$$

Доказать.

§ 16. Квадратичные иррациональности и периодические непрерывные дроби

Определение. Иррациональность называется квадратичной, если она удовлетворяет квадратному уравнению с целыми коэффициентами (вообще говоря, с рациональными коэффициентами). Общий вид квадратичной иррациональности: $\frac{a+\sqrt{b}}{c}$, где a, $c \neq 0$ и $b > 0$—целые числа.

Теорема. Квадратичные и только квадратичные иррациональности разлагаются в периодическую непрерывную дробь.

404. Свернуть периодические непрерывные дроби: 1) $(\overline{2,3})$; 2) $(\overline{1,1,2,2})$; 3) $(\overline{3,4,5,2,1})$; 4) $(1,2,3,\overline{4})$; 5) $(0,1,1,1,1,\overline{2,2,2})$; 6) $(a, \overline{a, 2a})$.

405. Найти иррациональность α, если:

1) $\frac{P_k}{Q_k}=\frac{10}{3}$, $\alpha_{k+1}=\sqrt{2}$; 2) $\frac{P_k}{Q_k}=\frac{37}{13}$, $\alpha_{k+1}=\frac{1+\sqrt{3}}{2}$.

406. Найти общий вид квадратичных иррациональностей, разлагающихся в непрерывную дробь с равными неполными частными.

407. Разложить в непрерывную дробь: 1) $\sqrt{x^2+1}$; 2) $\sqrt{a^4+2a}$.

408. Доказать, что положительный корень трехчлена

$$bx^2-abx-a,$$

где a и b — натуральные числа, разлагается в чистую периодическую непрерывную дробь с длиной периода, равной 2. Верна ли обратная теорема?

409. Доказать теорему: если квадратное уравнение с целыми коэффициентами имеет корень $x=(\overline{a, b})$, то вторым его корнем служит $-\frac{1}{(\overline{b, a})}$.

410. Если положительная квадратичная иррациональность разлагается в чистую периодическую непрерывную дробь, то сопряженная ей иррациональность принадлежит интервалу $(-1, 0)$. Доказать.

411. Доказать теорему: если квадратное уравнение с целыми коэффициентами имеет корень $x=(a, \overline{b, c})$, то второй его корень есть $a-\overline{(c, b)}$.

412. Найти произведение непрерывных дробей $(\overline{a, b})$ и $(0, \overline{b, a})$.

413. Доказать, что числа $\alpha=(a, b, c)$ и $\beta=(c, b, a)$ пропорциональны числам $x=(\overline{a, b, c})$ и $y=(\overline{c, b, a})$.

414. Доказать, что иррациональность вида $\sqrt{m}$ (m — число натуральное) разлагается в непрерывную дробь, период которой начинается со второго неполного частного.

§ 17. Алгебраические и трансцендентные числа

Комплексное число называется алгебраическим, если оно является корнем некоторого многочлена с целыми коэффициентами (вообще говоря, с рациональными коэффициентами). В противном случае комплексное число называется трансцендентным.

Натуральное число n называется порядком (степенью или высотой) алгебраического числа, если последнее является корнем многочлена n-й степени с целыми коэффициентами, но не является корнем многочлена степени $(n-1)$-й с целыми коэффициентами.

Теорема Лиувилля. Для каждого действительного алгебраического числа α порядка n существует $c>0$, такое, что $\left|\alpha-\frac{a}{b}\right|>\frac{c}{b^n}$, для всех рациональных чисел $\frac{a}{b}$ отличных от α.

Следствие. Иррациональные числа $\alpha=(q_0, q_1, q_2, \ldots)$, где $q_n>(Q_{n-1})^{n-1}$ и $n=1, 2, 3, \ldots$, являются трансцендентными.

Все числа вида α^β, где α и β — числа алгебраические, причем $\alpha\neq 0$; 1 и β — порядка $\geqslant 2$, являются трансцендентными (теорема Гельфонда).

В уравнении $y=e^x$ числа x и y не могут быть оба алгебраическими, за исключением случая, когда $x=0$ и $y=1$ (теорема Линдемана).

415. Доказать, что следующие числа являются алгебраическими: 1) $\sqrt[4]{4-\sqrt[3]{2}}$; 2) $\sqrt{2}+\sqrt[3]{3}$; 3) $a+\sqrt[n]{b}$;

4) $a+i\sqrt{b}$ (a и b — числа рациональные); 5) $\cos\frac{\pi}{n}+$ $+i\sin\frac{\pi}{n}$; 6) $\sin 10^0$.

416. Указать порядок алгебраических чисел: 1) $a+bi$ (a, b — рациональные); 2) $\sqrt[3]{3}$; 3) $\sqrt[3]{2}-1$; 4) $\sqrt{2}-\sqrt{3}$.

417. Доказать, что корни уравнений: а) $x^3+2\sqrt{2}x^2+$ $+2=0$ и б) $x^2+2ix+10=0$ — являются числами алгебраическими.

418. Доказать, что корни уравнения x^5-3x^2+12x- $-6=0$ есть алгебраические числа пятого порядка.

419. Построить хотя бы одно трансцендентное число способом Лиувилля.

420. Доказать, что число $\alpha=\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\ldots$ (число Лиувилля) является трансцендентным.

421. С помощью теоремы Гельфонда доказать трансцендентность чисел: 1) $\lg 2$; 2) $\log_2 10$; 3) $\ln 5$.

С помощью теоремы Линдемана доказать трансцендентность числа $\frac{\lg a}{\lg e}$, где a — число алгебраическое.

ГЛАВА 4

ЧИСЛОВЫЕ ФУНКЦИИ

§ 18. Целая часть действительного числа

Целая часть действительного числа x, т. е. $[x]$, определяется либо двойным неравенством $[x]\leqslant x<[x]+1$ или $x-1<[x]\leqslant x$, либо равенством $x=[x]+\alpha$, $0\leqslant\alpha<1$.

Если хотя бы одно из чисел x_1 и x_2 целое, то $[x_1+x_2]=[x_1]+[x_2]$.

Имеет место тождество $\left[\frac{x}{m}\right]=\left[\frac{[x]}{m}\right]$.

Показатель степени, с которым простое число p входит в каноническое разложение $m!$, равен $\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\ldots+\left[\frac{m}{p^s}\right]$, где s определяется соотношением $p^s\leqslant m<p^{s+1}$.

422. Найти целую часть чисел: 1) $-2{,}7$; 2) $2+\sqrt[3]{987}$; 3) $\frac{7-\sqrt{21}}{2}$; 4) $\frac{10}{3+\sqrt{3}}$; 5) $1{,}(3)+2\operatorname{tg}\frac{\pi}{4}$; 6) $3+\sin\frac{13\pi}{7}$; 7) $3-2\cos\frac{90\pi}{181}$; 8) $2-\lg 2512$; 9) $2-\lg\overline{abcd}$; 10) $\sqrt{30}+\sqrt[3]{10}$.

423. Доказать, что $[\pi]^{[e]}+[e]=[e]^{[\pi]}+[\pi]$, где $\pi=3{,}14\ldots$ — отношение длины окружности к ее диаметру и $e=\lim\limits_{n\to\infty}\left(1+\frac{1}{n}\right)^n=2{,}7\ldots$.

424. Доказать, что $\left[\frac{p}{4}\right]$, где $p>2$ — число простое, равно либо $\frac{p-1}{4}$, либо $\frac{p-3}{4}$.

425. Доказать, что $\left[\frac{a}{m}\right]=\frac{a-r}{m}$, где r — остаток от деления a на m.

426. Доказать, что $\left(\frac{2}{p}\right)=(-1)^{\left[\frac{p+1}{4}\right]}$, где $\left(\frac{2}{p}\right)$ — символ Лежандра.

427. Доказать, что $\frac{[nx]}{n} \leqslant x < \frac{[nx]}{n} + \frac{1}{n}$, $n=1, 2, \ldots$.

428. Доказать, что $\left[\frac{x+y}{n}\right]$ равно либо $\left[\frac{x}{n}\right]+\left[\frac{y}{n}\right]$, либо $\left[\frac{x}{n}\right]+\left[\frac{y}{n}\right]+1$.

429. При помощи знака целой части записать число единиц второго разряда, содержащихся в числе m.

430. Если m — число нечетное, то $\left[\frac{m}{2}\right]=\frac{m-1}{2}$. Доказать.

431. Построить графики функций: а) $\left[-\frac{x}{2}\right]$; б) $\left[\frac{x^2}{2}-1\right]$; в) $[\sin x]$.

432. Решить уравнения: 1) $[x^2]=2$; 2) $[3x^2-x]=x+1$; 3) $[x]=\frac{3}{4}x$; 4) $[x^2]=x$.

433. Доказать, что не существует натуральных чисел m, удовлетворяющих уравнению $[12,4m]=87$.

434. Установить зависимость между функциями $[-x]$ и $[x]$.

435. Найти числа, логарифмы которых имеют характеристику -2.

436. Доказать, что $[x_1+x_2+\ldots+x_n] \geqslant [x_1]+[x_2]+\ldots+[x_n]$.

437. Доказать, что $[nx] \geqslant n[x]$, $n=1, 2, 3, \ldots$.

438. Сколько натуральных чисел, кратных 786, заключено между 10^6 и 10^7?

439. Сколько натуральных чисел, меньших 1000, не делятся ни на 5, ни на 7?

440. Найти число натуральных чисел, не превышающих 100 и взаимно простых с 36.

441. Сколькими нулями оканчивается число 1964!?

442. С каким показателем степени входит простое число p в каноническое разложение $p^n! = 1 \cdot 2 \cdot 3 \ldots p^n$?

443. С каким показателем степени число 6 входит в произведение 100!?

444. Найти каноническое разложение числа $11! = 1 \cdot 2 \cdot 3 \ldots 11$.

445. Найти каноническое разложение числа $\frac{20!}{10!\,10!}$.

446. Найти наибольшее натуральное число a, при котором $N = \frac{101 \cdot 102 \ldots 1000}{7^a}$ — число целое.

447. Найти показатель степени, с которым простое число p входит в каноническое разложение числа: 1) $(2m)!!$; 2) $(2m+1)!!$

448. Доказать, что для записи натурального числа N в системе счисления с основанием g требуется $[\log_g N]+1$ знаков. Пользуясь этой формулой, найти натуральные числа, которые в двоичной системе счисления являются пятизначными. Из скольких знаков, в десятичной системе счисления, состоит число 12^{100}?

449. Вывести формулу для функции $Q_n(x)$, выражающей число n-х степеней натуральных чисел, не превышающих действительное число $x>0$.

450. Найти НОК всех натуральных чисел, не превышающих m.

451. Сколько всего точек с целочисленными координатами заключено на криволинейной трапеции $a \leqslant x \leqslant b$, $0 \leqslant y \leqslant f(x)$, где a и b — натуральные числа и $f(x)$ — неотрицательная непрерывная на указанном отрезке функция?

452. Сколько всего точек с целочисленными координатами заключено на круге $x^2+y^2=6{,}5^2$?

453. Доказать, что $\left[\frac{a}{4}\right] + \left[\frac{2a}{4}\right] + \left[\frac{3a}{4}\right] = \frac{3(a-1)}{2}$, если $(a, 4)=1$.

454. Доказать, что $\left[\frac{a}{m}\right] + \left[\frac{2a}{m}\right] + \ldots + \left[\frac{(m-1)a}{m}\right] = \frac{(m-1)(a-1)}{2}$, если $(a, m)=1$, $m \geqslant 2$ и $a \geqslant 2$.

455. Доказать, что $[x]+\left[x+\frac{1}{2}\right]=[2x]$. Дать графическую иллюстрацию.

456. Найти значения x, при которых имеет место равенство $[x]-2\left[\frac{x}{2}\right]=1$.

457. Решить уравнение $\left[\frac{x}{m}\right] = \left[\frac{x}{m-1}\right]$, $m=2, 3, 4, \ldots$.

458. Найти условие существования решения уравнения вида $[ax^2+bx+c]=d$, где $a \neq 0$ и d — число целое.

459. Доказать, что $\left[\frac{4}{p}\right]+\left[\frac{8}{p}\right]+\left[\frac{12}{p}\right]+\ldots+$ $+\left[\frac{2(p-1)}{p}\right]=\left[\frac{p+1}{4}\right]$, где p — нечетное простое число.

§ 19. Число и сумма делителей натурального числа

По определению $\tau(1)=\sigma(1)=1$. При $m>1$ данные функции вычисляются по формулам:

$$\tau(m)=\prod_{i=1}^{k}(1+\alpha_i) \text{ и } \sigma(m)=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}, \quad \text{где}$$

$\prod_{i=1}^{k} p_i^{\alpha_i}$ — каноническое разложение m.

Обе функции мультипликативны, т. е. если $(m, n)=1$, то $\tau(mn)=\tau(m)\tau(n)$ и $\sigma(mn)=\sigma(m)\sigma(n)$.

460. Найти число и сумму делителей 600.

461. Найти все делители чисел 90 и 360.

462. Построить графики функций $y=\tau(x)$ и $y=\sigma(x)$, где $x=1, 2, 3, \ldots$.

463. Доказать, что для каждой пары простых чисел-близнецов $p_1<p_2$ имеет место равенство $\sigma(p_1)=\varphi(p_2)$.

464. Доказать, что существует бесконечное множество натуральных чисел m, таких, что $\sigma(m)=2m-1$.

465. Доказать, что функции $\tau(m)$ и $\sigma(m)$ мультипликативны, т. е. что при $(m, n)=1$ имеют место равенства $\tau(m_1m_2)=\tau(m_1)\tau(m_2)$ и $\sigma(m_1m_2)=\sigma(m_1)\sigma(m_2)$.

466. $(m, n)>1$. Что больше: $\tau(mn)$ или $\tau(m)\tau(n)$? Рассмотреть этот же вопрос относительно функции $\sigma(x)$.

467. Доказать, что числа $\tau(m^n)$ и n — взаимно простые.

468. Вывести формулу для функции $\delta(m)$ — произведения всех натуральных делителей натурального числа m. Найти $\delta(10)$.

469. $m=1968$. Найти $\varphi(m)$, $\tau(m)$, $\sigma(m)$ и $\delta(m)$.

470. Доказать, что множество всех натуральных чисел, равных произведению всех своих натуральных делителей, совпадает с множеством всех простых чисел.

471. Найти натуральное число, произведение всех делителей которого равно 5832.

472. Найти формулу функции $s_n(m)$, выражающей сумму n-х степеней всех натуральных делителей натуральных делителей натурального числа m (n — число целое).

Замечание. Конечно, $s_n(m)=\sum_{i=1}^{\tau(m)} d_i^n$, где d_i—все-возможные делители m, но этот общий вид формулы не имеет практического значения. Полезно обратить внимание на то, что $s_0(m)=\sum_{i=1}^{\tau(m)} 1=\tau(m)$ и $s_1(m)=\sum_{i=1}^{\tau(m)} d_i=$ $=\sigma(m)$.

473. Доказать, что число 8128 является совершенным. Натуральное число m называется совершенным, если $\sigma(m)=2m$; недостаточным, если $\sigma(m)<2m$, и избыточным, если $\sigma(m)>2m$.

474. Доказать, что любая натуральная степень простого числа является числом недостаточным.

475. Доказать, что нечетное натуральное число с двумя простыми делителями — недостаточное.

476. Доказать теорему Евклида: четные натуральные числа вида $2^\alpha(2^{\alpha+1}-1)$, где $2^{\alpha+1}-1$ — число простое, являются совершенными.

477. Доказать, что натуральные числа вида $2^\alpha(2^{\alpha+1}-$ $-1)$, где $2^{\alpha+1}-1$ — число простое, являются единственными четными совершенными числами (теорема Эйлера).

478. Найти наименьшее число вида $2^\alpha\cdot p_1p_2$, где p_1 и p_2 — нечетные простые числа, сумма делителей которого втрое больше самого числа (задача Ферма).

479. Найти натуральное число, зная, что оно имеет два простых делителя, всего 6 делителей, сумма которых 28.

480. Найти натуральное число, если оно делится на 3 и на 4 и имеет 14 делителей.

481. Некоторое натуральное число имеет два простых делителя. Его квадрат имеет всего 15 делителей. Сколько делителей имеет куб этого числа?

482. Некоторое натуральное число имеет два простых делителя. Его квадрат имеет всего 81 делитель. Сколько делителей имеет куб этого числа?

483. Найти число вида $m=2^x\cdot 3^y\cdot 5^z$, зная, что половина его имеет на 30 делителей меньше, треть — на 35 и пятая часть — на 42 делителя меньше, чем само число.

484. Доказать, что натуральное число является точным квадратом тогда и только тогда, когда число его различных натуральных делителей нечетное.

§ 20. Число простых чисел, не превышающих данное положительное число

Функция $\pi(x)$, выражающая число простых чисел, не превышающих $x>0$, возрастает неограниченно с возрастанием x. Существуют постоянные $a<b$, такие, что при всех $x>2$ имеют место неравенства $a<\pi(x):\frac{x}{\ln x}<b$ (неравенства Чебышева). Более точно связь между функциями $\pi(x)$ и $\frac{x}{\ln x}$ выражается равенством $\lim\limits_{x\to\infty}\left[\pi(x):\frac{x}{\ln x}\right]=1$ или асимптотической формулой $\pi(x)\sim\frac{x}{\ln x}$.

485. Построить график функции $y=\pi(x)$. Решить графически уравнение $\pi(x)=\frac{x}{2}$.

486. По формуле $\pi(x)=\frac{x}{\ln x}$ найти приближенное значение $\pi(1000)$ и указать относительную погрешность результата.

487. При помощи неравенства Чебышева доказать, что $\frac{\pi(x)}{x}\to 0$ $(x\to+\infty)$.

488. Доказать, что $\frac{\pi(p-1)}{p-1}<\frac{\pi(p)}{p}$, но $\frac{\pi(m)}{m}<\frac{\pi(m-1)}{m-1}$, если m — число составное.

ГЛАВА 5

ДО СИХ ПОР НЕ РЕШЕННЫЕ ЗАДАЧИ ТЕОРИИ ЧИСЕЛ

Науку о числах двигает вперед не только то, что о них известно, но и выяснение того, что еще неизвестно. Ниже приводится несколько простых по формулировке задач теории чисел, до сих пор не имеющих своего решения. Одни из них возникли очень давно, другие — сравнительно недавно. Интересно, что, по-видимому, со временем число нерешенных задач возрастает, так как быстрее появляются новые, чем решаются уже поставленные.

1. Хорошо известны формулы: четного числа ($N=2n$), нечетного числа ($N=2n+1$), квадратного числа ($N=n^2$) и формулы ряда других целых чисел (т. е. аналитические выражения функций, множества значений которых являются классом целых чисел, обладающих некоторым заданным свойством).

Однако до сих пор неизвестна формула простого числа (т. е. аналитическое выражение функции, множество значений которой является классом всех простых чисел). Правда, существует формула, несколько лет назад полученная в Советском Союзе Л. С. Вешеневским (см., например, журнал «Математика в школе», 1962, № 5, стр. 74), но она очень сложна.

2. В связи с поисками формулы простого числа возникли другие задачи, решение которых еще неизвестно. Приведем две из них.

Существуют функции, для многих последовательных натуральных значений аргумента, дающие простые числа. Наиболее популярной из них является «многочлен Эйлера»: $f(x)=x^2+x+41$, который при $x=0, 1, \ldots, 39$ дает простые числа 41, 43, . . . , 1601.

Предполагают, что существует бесконечное множество значений x (конечно, натуральных), которым соответствуют простые числа вида $f(x)=x^2+x+41$.

Неизвестно, существуют ли натуральные числа $m>41$, для которых все числа вида $f(x)=x^2+x+m$, где $x=1, 2, 3, 4, \ldots, m-2$, являются простыми.

3. Простые числа Ферма $F_n=2^{2^n}+1$, где $n=0, 1, 2, \ldots$ (Ферма ошибочно предполагал, что все числа такого вида простые), играют известную роль в геометрии: как доказал Гаусс, при помощи циркуля и линейки можно разделить окружность только на $2^m F_n$ равных частей, где $F_n=2^{2^n}+1$ — число простое. Легко проверить, что при $n=0, 1, 2, 3, 4$ число F_n является простым. Но уже при $n=5$ (как впервые обнаружил Эйлер) оно является составным (см. задачу 357).

Сравнительно недавно высказано предположение, что при $n\geqslant 5$ все числа F_n являются составными.

Сложнее будет ответить на вопрос, является ли множество составных (простых) чисел вида F_n бесконечным?

4. Уже Евклид знал, что не существует наибольшего простого числа, но до сих пор этот вопрос остается открытым относительно простых чисел некоторых определенных видов, например вида n^2+1 ($n=1, 2, 3, \ldots$): неизвестно, является ли множество простых чисел данного вида (2, 5, 17, 37, ...) бесконечным.

5. Открытым остается вопрос и о существовании пары наибольших простых чисел-близнецов (2 и 3, 3 и 5, 5 и 7, 11 и 13, ...).

Отметим, что вопрос о «близнецах» равносилен вопросу: имеет ли уравнение $x-y=2$ бесконечное множество решений в простых числах.

6. При доказательстве бесконечности множества всех простых чисел обычно рассматриваются числа вида $\psi(k)=p_1p_2\ldots p_k+1$, где p_i $(i=1, 2, \ldots, k)$ — первые k простых чисел. Легко непосредственно установить, что число $\psi(k)$ может быть как простым, так и составным (см. задачу 69). Однако мы не знаем, является ли множество всех простых (составных) чисел $\psi(k)$ бесконечным (конечным).

7. Ясно, что разность двух нечетных простых чисел есть число четное. Неизвестно, верна ли обратная теорема, т. е. можно ли любое четное число представить в виде разности двух простых чисел.

8. Ясно также, что любое простое число заключено между двумя последовательными квадратными числами (2 и 3 — между 1 и 4; 5 и 7 — между 4 и 9 и т. д.). Однако неизвестно, верна ли обратная теорема, т. е. всегда

ли между двумя последовательными квадратными числами заключено по крайней мере одно простое число.

9. Решение уравнений в целых числах имеет не только теоретический интерес. Эта задача иногда встречается в физике. С нею связано много частных задач, решение которых неизвестно. Из них в литературе наиболее часто упоминается «великая теорема Ферма»: уравнение $x^n+y^n=z^n$ $(n\geqslant 3)$ не имеет решений в целых числах. В настоящее время эта теорема доказана для многих значений n, но ее доказательство в общем виде остается неизвестным.

10. Неизвестно также, существует ли прямоугольный параллелепипед, у которого все ребра и диагонали боковых граней выражаются натуральными числами, т. е. разрешимо ли в натуральных числах уравнение $x^2+y^2+2z^2=$ $=u^2+v^2$.

11. Мы не знаем, существуют ли натуральные числа $x>1$, $y>1$, удовлетворяющие уравнению $\sum\limits_{i=1}^{x-1} i^y=x^y$.

12. Известно, что уравнение $x^3-y^2=7$ имеет конечное число решений в целых числах, в частности следующие решения: $x=2$, $y=\pm 1$; $x=32$, $y=\pm 181$. Но сколько именно целочисленных решений имеет это уравнение и каковы все эти решения, пока неизвестно.

13. Ряд нерешенных задач относится к числовым функциям. Например, справедливость равенства $\left[\frac{3^n}{2^n}\right]=$ $=\left[\frac{3^n}{2^n-1}\right]$, где $n>2$ — число натуральное, проверено советским математиком В. А. Голубевым для всех $3\leqslant n\leqslant$ $\leqslant 150$. Однако, является ли это равенство тождеством относительно n, неизвестно.

14. Легко убедиться в том, что уравнение $\tau(m)=$ $=\tau(m+1)$ имеет решения (для этого достаточно рассмотреть график данной функции; задача 462). Но мы не знаем ответа на вопрос, имеет ли это уравнение бесконечное множество решений.

Однако известно, что в случае положительного ответа на этот вопрос можно было бы утверждать, что существует бесконечное множество натуральных чисел m, для которых $\tau(m)=\tau(m+1)=4$, т. е. таких пар последовательных натуральных чисел, каждое из которых является произведением двух простых чисел (например, $\tau(21)=$ $=\tau(22)=4$, где $21=3\cdot7$ и $22=2\cdot11$).

15. Аналогичную не имеющую решения задачу можно привести относительно функции $\sigma(m)$: сколько решений имеет уравнение $\sigma(m)=\sigma(m+1)$?

16. Легко доказать, что уравнение $\sigma(m)=2m-1$ имеет бесконечное множество решений (см. задачу 464). Но неизвестно, имеет ли решение уравнение $\sigma(m)=2m+1$.

17. В настоящее время сравнительно хорошо известно множество всех четных совершенных чисел (см. задачи 473—476), но совершенно неизвестно, существуют ли нечетные совершенные числа. Интересно, что установлены некоторые свойства нечетных совершенных чисел при условии их существования (в частности, советскими математиками А. С. Турчаниновым и И. С. Градштейном).

18. Существуют дружественные натуральные числа, т. е. такие натуральные числа m и n, для которых $\sigma(m)=$ $=\sigma(n)=m+n$ (например, $\sigma(220)=\sigma(284)=220+284$). В настоящее время никто не может ответить на вопрос, существуют ли дружественные числа, из которых одно — четное, а другое — нечетное?

19. Из таблиц значений функции Эйлера видно, что каждое из встречающихся в этих таблицах значений данная функция принимает по крайней мере дважды. Однако все попытки доказать, что для любого натурального числа m существует другое натуральное число n, для которого $\varphi(n)=\varphi(m)$, пока встречают непреодолимые трудности. Для некоторых частных случаев утверждение верно. Например, если m — число нечетное, то $\varphi(2m)=$ $=\varphi(m)$; если число вида 2^n+1 простое, то $\varphi(2^{n+1})=$ $=\varphi(2^n+1)=2^n$.

20. В настоящее время никто не может доказать (или опровергнуть) утверждение, что для всех натуральных чисел $m>1$ и $n>1$ имеет место неравенство $\pi(m+n)\leqslant$ $\leqslant\pi(m)+\pi(n)$.

21. Задачи третьей главы данного сборника («Непрерывные дроби») относятся к разложению в непрерывную дробь рациональных чисел и квадратичных иррациональностей. Это не случайно. Свойства непрерывных дробей, соответствующих алгебраическим иррациональностям степени выше второй, совершенно неизвестны.

ОТВЕТЫ, УКАЗАНИЯ И РЕШЕНИЯ

1. 1) 7 и 150; 2) 1 и 0; 3) 0 и 100; 4) $\left[\frac{-4}{2}\right]=-2$ и 2; 5) 3 и 4; 6) 4411 и 3; 7) 220 и 1; 8) — 11 и 3.

2. 1) По модулю 3 остаток может иметь значения: $r=0$; 1; 2. По формуле $a=3\cdot(-2)+r$ находим соответствующие значения делимого: $a=-6$; -5; -4; 2) 202; 210; 211; 212; 220 (в троичной системе счисления); 3) -21; -20; -13; -12; -11; -10; -3; -2; -1 (в системе счисления с основанием 4).

3. Искомое число a должно удовлетворять соотношению $a=13\cdot 17+r$, $0\leqslant r\leqslant 12$. Отсюда ясно, что наибольшее значение a соответствует наибольшему значению r, т. е. $r=12$. Имеем: $a=13\cdot 17+12=233$.

4. 1) $25=m\cdot 3+r$ или, $r=25-3m$. По определению остатка имеем: $0\leqslant 25-3m<m$, откуда $m=7$; 8. Следовательно, $r=2$; 6. 2) $m=8$; 9 и $r=2$; 6.

5. 1) $(2n+1)^2=4n(n+1)+1$, где $n(n+1)\ \vdots\ 2$. 2) $n^2+(n+1)^2=2n(n+1)+1$.

6. $p=6q+r$ $(0\leqslant r\leqslant 5)$. При $r=0$; 2; 3; 4 число вида $6q+r$ либо составное, либо простое, меньше 5.

7. По модулю 6 либо $p=6q+1$, либо $p=6q+5$. В первом случае $p^2=24q^2+12q(q+1)+1=24q^2+24Q+1$. Во втором случае $p^2=(24q^2+48q+24)+(12q^2+12q)+1=24Q_1+24Q_2+1$.

8. Если $a_1=mq_1+1$ и $a_2=mq_2+1$, то $a_1a_2=m^2q_1q_2+m(q_1+q_2)+1=mQ+1$ (Q — число целое). Этот вывод допускает обобщение: если $a_i=mq_i+1$ $(i=1, 2, \ldots, n)$, то $\prod\limits_{i=1}^{n} a_i=mQ+1$. Докажите.

9. Чтобы доказать неразрешимость уравнения $3m+2=x^2$ в натуральных числах, достаточно исследовать классы значений x по модулю 3: $x=3q$, $x=3q+1$ и $x=3q+2$ (q — число целое).

10. Допустимые значения g легко уточнить: $7\leqslant g\leqslant 11$. Непосредственная проверка показывает, что $g=7$. Будет ли решение задачи единственным, если снять ограничение $g\leqslant 11$?

11. $15=7\cdot 2+1$; если $15^n=7q+1$, то $15^{n+1}=15^n\cdot 15=7Q+1$ (теорема задачи 8).

12. 1) $2^{2^2}+1=17$; если $2^{2^n}+1=10q+7$, то $2^{2^{n+1}}+1=2^{2^n\cdot 2}+1=(2^{2^n})^2+1=(10q+6)^2+1=(10Q+6)+1=10Q+7$.

13. $(2q_1+1)^2+(2q_2+1)^2=4Q+2$, т. е. исследуемая сумма, будучи числом четным, не делится на 4.

14. Если оба катета x и y не делятся на 3, то каждый из них есть число вида $3q+1$ либо $3q+2$, откуда $x^2+y^2=(3Q_1+1)+(3Q_2+1)=3Q+2$. Это означает, что квадрат гипотенузы, а следовательно и сама гипотенуза, не делится на 3. Однако в этом случае ее квадрат при делении на 3 должен давать остаток 1, но не 2 (задача 9), как получено выше. Следовательно, либо $x \vdots 3$, либо $y \vdots 3$.

15. Если катет x не $\vdots$ 5, то $x=5q+r$, $1\leqslant r\leqslant 4$, откуда либо $x^2=5Q+1$, либо $x^2=5Q+4$. Если и катет y не $\vdots$ 5, то точно также либо $y^2=5t+1$, либо $y^2=5t+4$. Но тогда $x^2+y^2=5k+r$, $r=0$; 2; 3. Из трех возможностей для r имеет место лишь $r=0$, так как если гипотенуза не $\vdots$ 5, то ее квадрат при делении на 5 дает остаток либо 1, либо 4 (но не 2 и не 3). Аналогично из допущения, что катет и гипотенуза не $\vdots$ 5, можно вывести, что второй катет $\vdots$ 5.

16. $n=5k+1$ и $n=5k+3$, где $k=0, 1, 2, \ldots$.

17. $ax-by=ax-bx+bx-by=x(a-b)+b(x-y)$.

18. $4^n+15n-1=(1+3)^n+15n-1=1+3n+9Q+15n-1=18n+9Q$, где Q — число натуральное.

19. 1) $f(1)=27$; если $f(n)=27q$, то $f(n+1)=27q+9(10^n+2)$, где $(10^n+2) \vdots 3$, так как сумма цифр этого числа кратна 3. 2) $F(1)=256 \vdots 64$. Если $F(n)=64q$, то $F(n+1)=64q+8(3^{2n+3}+5)$. Докажем, что $\varphi(n)=3^{2n+3}+5$ кратно 8. Действительно, $\varphi(1)=248 \vdots 8$, и если $\varphi(n)=8k$, то $\varphi(n+1)=8q+8\cdot 3^{2n+3}$.

20. 1) $(n, 2n^2+1)=1$. Очевидно, что $f(n)=2n^2+1$ не $\vdots$ 2. Остается доказать, что $f(n)$ не $\vdots$ 5. Имеем: $f(5q+r)=5Q+f(r)$, где $r=0, 1, 2, 3, 4$, и $f(r)$ не $\vdots$ 5 (в последнем легко убедиться непосредственно).

21. Если $N_1=\overline{abc}$ и $N_2=\overline{def}$, то $\overline{abcdef}=N_1\cdot 10^3+N_2=(N_1+N_2)+999N_1$, где $999=37\cdot 27$.

22. 1) $m^5-m|_{m=5x+y}=5q+y^5-5x-y=5Q+y(y^4-1)$, где $0\leqslant y\leqslant 4$. Непосредственной проверкой можно убедиться, что $y(y^4-1) \vdots 5$. 2) При $m=6x+y$, $0\leqslant y\leqslant 5$, имеем: $m(m^2+5)=(6x+y)(6q+y^2+5)=6Q+y^3+5y$, где $y^3+5y \vdots 6$, как нетрудно проверить.

23. $N=1000q+r=1001q+r-q$, откуда $N \vdots 7$, 11 или 13 тогда и только тогда, когда разность между числом его тысяч и остатком от деления его на 1000 делится соответственно на 7, 11 или на 13. При $N=368\,312$ упомянутая разность $368-312=56$ делится на 7, но не делится ни на 11, ни на 13. Следовательно, $368\,312 \vdots 7$, но не $\vdots$ 11 и не $\vdots$ 13.

24. Пусть $N_1=\overline{a_n \ldots a_1a_0}$ и $N_2=\overline{b_m \ldots b_1b_0}$. Так как $N_1=9Q_1+\sum a_i$ и $N_2=9Q_2+\sum\limits_{j=1}^{m} b_j$, где $\sum a_i=\sum b_j$, то $N_1-N_2=9(Q_1-Q_2)$.

25. $k+(k+1)+\ldots+(k+2n)=(k+n)(2n+1)$.

26. $\dfrac{(2n+1)^2-(2k+1)^2}{(2n+1)^2+(2k+1)^2}=\dfrac{4(n-k)(n+k-1)}{2[2(n^2+k^2+n+k)+1]}$.

27. Пусть $N=\overline{abc}$. Тогда $N_1=\overline{bca}=\overline{bc0}+a=\overline{abc0}+a-a\cdot 10^3=$ $=10N-37\cdot 27a$ и $N_2=\overline{cab}=\overline{c00}+\overline{ab}=\overline{abc\,00}+\overline{ab}-\overline{ab}\cdot 10^3=100N-$ $-37\cdot 27\cdot \overline{ab}$.

28. $\overline{aaa}\ \vdots\ 3$, так как $a+a+a=3a\ \vdots\ 3$. Если $\underbrace{\overline{aa\ldots a}}_{3^n\text{цифр}}\ \vdots\ 3^n$, то

$$\underbrace{\overline{aa\ldots a}}_{3^{n+1}\text{цифр}}=\overline{\underbrace{aa\ldots a}_{3^n\text{цифр}}\ \underbrace{aa\ldots a}_{3^n\text{цифр}}\ \underbrace{aa\ldots a}_{3^n\text{цифр}}}=\underbrace{\overline{aa\ \ldots\ a}}_{3^n\text{цифр}}\cdot(10^{3^n})^2+$$
$$+\underbrace{\overline{aa\ldots a}}_{3^n\text{цифр}}\cdot 10^{3^n}+\underbrace{\overline{aa\ldots a}}_{3^n}=\overline{aa\ldots a}\cdot 100\ldots 01\,00\ldots 01\ \vdots\ 3^{n+1}.$$

29. 1) 3 и 88 200; 2) 23 и 28 956 931.

30. 1) $(6, 35)=(6, 143)=(35, 143)=1$; 2) $(n, n+1)=1$.

31. $(2n, 2n+2)=2(n, n+1)=2$ и $(2n+1, 2n+3)=1$; последнее можно проверить при помощи алгоритма Евклида.

32. $(cb, bc, ca)=c\cdot(a, b)$. С другой стороны, $(a, b, c)=$ $=((a, b), c)=d$, откуда $(a, b)=dx$ и $c=dy$. Следовательно, $(cb, bc, ca)=d^2xy$.

33. Пусть $(a+b, a-b)=d$, тогда $a+b=dx$ и $a-b=dy$, откуда $2a=d(x+y)$ и $2b=d(x-y)$. Следовательно, $d=OD(2a, 2b)$. Но $(2a, 2b)=2$; поэтому $2\ \vdots\ d$ и либо $d=1$, либо $d=2$.

34. Пусть $(a, a+b)=d$, тогда $a=dx$ и $a+b=dy$ или $dx+b=dy$, откуда $b\ \vdots\ d$ и $d=OD(a, b)$, откуда $d=1$. Дробь $\dfrac{a}{a+b}$ несократима.

35. Если a и b — числа нечетные, то $(a, b)=d$ — число нечетное. По условию $2^n\ \vdots\ d$, откуда $d=1$.

36. 1) $(d, m)=(d, [dx, dy])=d(1, [x, y])=d$. Результат не изменится, если считать, что $d=(a_1, a_2, \ldots, a_n)$ и $m=[a_1, a_2, \ldots, \ldots, a_n]$. 2) $(ab, m)=(dm, m)=m\cdot(d, 1)=m$, где $d=(a, b)$. 3) Если $p=OD(a+b, ab)$, то либо $a\ \vdots\ p$, либо $b\ \vdots\ p$. Но тогда в силу $a+b\ \vdots\ p$ число p должно быть $OD(a, b)$, что противоречит условию $(a, b)=1$. Итак, при $(a, b)=1$ имеем $(a+b, ab)=1$. 4) Пусть $(a, b)=d$ и $a=dx$, $b=dy$, где $(x, y)=1$. Тогда $(a+b, m)=(d(x+y), dxy)=$ $=d(x+y, xy)=d$. Следовательно, $(a+b, [a, b])=(a, b)$.

37. 1) 1. 2) Пусть $(10n+9, n+1)=d$ и $10n+9=dx$, $n+1=dy$. Тогда $10(dy-1)+9=dx$ или $10dy-1=dx$, откуда $d=1$. 3) Если $(3n+1, 10n+3)=d$, то

$$\begin{cases}3n+1=dx,\\ 10n+3=dy,\end{cases}\quad\text{или}\quad\begin{cases}30n+10=10dx,\\ 30n+\ 9=\ 3dy,\end{cases}$$

откуда $1=d\cdot(10x-3y)$ и $d=1$.

Задачу можно решить и с помощью алгоритма Евклида.

38. Если $x=[a, b]=\dfrac{ab}{(a, b)}$, то $\left(\dfrac{x}{a}, \dfrac{x}{b}\right)=\left(\dfrac{b}{(a, b)}; \dfrac{a}{(a, b)}\right)=$ $=1$. Если $\left(\dfrac{x}{a}, \dfrac{x}{b}\right)=1$, то, положив $x=[a, b]\cdot y$, имеем: $\left(\dfrac{[a,b]y}{a}, \dfrac{[a, b]y}{b}\right)=y\left(\dfrac{b}{(a, b)}, \dfrac{a}{(a, b)}\right)=y=1$, откуда $x=[a, b]$.

39. Если $(a, b, c)=D$, то $a=Dx$, $b=Dy$, $c=Dz$, где x, y, z — числа нечетные, и $\dfrac{a+b}{2}=D\cdot\dfrac{x+y}{2}$, $\dfrac{a+c}{2}=D\cdot\dfrac{x+z}{2}$, $\dfrac{b+c}{2}=D\cdot\dfrac{y+z}{2}$, где $\dfrac{x+y}{2}$, $\dfrac{x+z}{2}$, $\dfrac{y+z}{2}$ — числа целые, откуда $D=OD\left(\dfrac{a+b}{2}, \dfrac{a+c}{2}, \dfrac{b+c}{2}\right)$. Положив $\left(\dfrac{a+b}{2}, \dfrac{a+c}{2}, \dfrac{b+c}{2}\right)=d$, имеем $d \vdots D$. С другой стороны, легкодоказать, что $d=OD(a, b, c)$, откуда $D \vdots d$. Таким образом, $D=d$.

40. Пусть $(a, b)=d$ и $a=dx$, $b=dy$, где $(x, y)=1$. Тогда $5a+$ $+3b=d(5x+3y)$ и $13a+8b=d(13x+8y)$, откуда $d=OD(5a+3b,$ $13a+8b)$. Остается доказать, что $(5x+3y, 13x+8y)=1$. Пусть $(5x+3y, 13x+8y)=\delta$ и

$$\begin{cases} 5x+3y=\delta n, \\ 13x+8y=\delta v, \end{cases}$$

откуда $x=\delta(8n-3v)$ и $y=\delta(5v-13n)$. Но $(x, y)=1$, поэтому $\delta=1$. Таким образом, $d=(5a+3b, 13a+8b)$.

41. $(n, n+1, n+2)=((n, n+1), n+2)=(1, n+2)=1$. Этот результат не изменится, если взять k последовательных натуральных чисел. $[n, n+1, n+2]=[[n, n+1], n+2]=[n(n+1), n+2]=$ $\dfrac{n(n+1)(n+2)}{(n(n+1), n+2)}=\dfrac{n(n+1)(n+2)}{(n, n+2)}$, но $(n, n+2)$ равен либо 1, либо 2 (в зависимости от четности n), поэтому $[n, n+1, n+2]$ равно либо $n(n+1)(n+2)$, либо $\dfrac{n(n+1)(n+2)}{2}$.

42. Если $nab=ax+by$, то $x=bk$ $(k=1, 2, 3, \ldots)$. При этих значениях x имеем $nab=abk+by$, откуда $y=a(n-k)$ и $k=1, 2, \ldots,$ $\ldots, (n-1)$ $(n>1)$. Итак, требуемое представление может иметь место при $k=1, 2, \ldots, n-1$ $(n>1)$. Так как $abk+ba(n-k)=nab$, то при $n>1$ требуемое представление действительно осуществимо, причем $n-1$ способами: $x=bk$, $y=a(n-k)$, где $k=1, 2, \ldots, n-1$.

43. Пусть $a=cq+r$, где $(c, r)=(a, c)=1$ и $b=cq_1+r_1$, где $(c, r_1)=(b, c)=1$. Тогда $ab=c\cdot Q+rr_1$, откуда $(ab, c)=(c, rr_1)=1$.

44. Пусть $a>b$ и $(a, b)=d$. Тогда $a=dx$ и $b=dy$, где $x-y>0$. Если $d>a-b=d(x-y)$ или $1>x-y$, то $0<x-y<1$, что невозможно, так как $x-y$ — число целое. Следовательно, $(a, b)\leqslant a-b$ $(a>b)$.

45. $ab \vdots (ab, c)$ и $bc \vdots (ab, c)$, поэтому $(ab, bc) \vdots (ab, c)$. Но $(ab, bc)=b\cdot(a, c)=b$; следовательно, $b \vdots (ab, c)$.

46. $c \vdots (ac, b)$ (см. предыдущую задачу), следовательно, $(c, b) \vdots$ $\vdots (ac, b)$; с другой стороны, $(ac, b) \vdots (c, b)$. Таким образом, $(ac, b)=$ $=(c, b)$.

47. Пусть $(mn, mk, nk)=d$. Так как $mnk \vdots d$, то существует целое число $x=\frac{mnk}{d}=m\cdot\frac{nk}{d}=n\cdot\frac{mk}{d}=k\cdot\frac{mn}{d}$, откуда $x=OK(m, n, k)$ и $x=[m, n, k]\cdot q$, $q\geqslant 1$. Таким образом, $\frac{[m, n, k]q}{m}=\frac{nk}{d}$, $\frac{[m, n, k]q}{n}=\frac{mk}{d}$ и $\frac{[m, n, k]q}{k}=\frac{mn}{d}$, откуда $q=OD\left(\frac{nk}{d}, \frac{mk}{d}, \frac{nm}{d}\right)=1$ и $x=[m, n, k]$.

48. 1) $(x, y)=30$ равносильно системе

$$\begin{cases} x=30u, \\ y=30v, \\ (u, v)=1, \end{cases}$$

поэтому первое уравнение данной системы дает $u+v=5$, откуда $u=1; 2; 3; 4$ и $x=30; 60; 90; 120$. Соответствующие значения y можно найти по формуле $y=150-x$. 2) При $x=45u$ и $y=45v$, где $(u, v)=1$, имеем $\frac{u}{v}=\frac{11}{7}$, откуда $u=11$ и $v=7$. Следовательно, $x=495$ и $y=315$. 3) При $x=20u$ и $y=20v$, где $(u, v)=1$, имеем $uv=21$, откуда $u=1; 3; 7; 21$ и $x=20; 60; 140; 420$. Соответствующие значения y легко найти по формуле $y=\frac{8400}{x}$. 4) $x=140$, $y=252$. 5) $x=2$, $y=10$ и $x=10$, $y=2$.

49. $qN=100q+bq=100q+a-a+bq=am-(a-bq)$, откуда и следует справедливость утверждения, так как $(q, m)=1$.

50. Пусть $N=10a+b$ и $m=10q+7$. Тогда $3m=10Q+1$, где $(Q, m)=1$, и $QN=3am-(a-bQ)$. Следовательно, $N \vdots m$ тогда и только тогда, когда $(a-bQ) \vdots m$.

51. $(q+1)N=10a(q+1)+b(q+1)=am+[a+b(q+1)]$, где $(q+1, 10q+9)=1$ (см. задачу 37).

52. Если $m=10q+3$, то $3m=10\cdot 3q+9$. Следует рассмотреть $(3q+1)N=(3q+1)(10a+b)=a\cdot 3m+[a+b(3q+1)]$, где $(3q+1, 10q+3)=1$ (см. задачу 37).

53. $10N_1=a_n \ldots a_2a_1\cdot 10+20a_0=N+19a_0$, где $(10, 19)=1$. Применение этого признака видно из следующей записи:

$$\begin{array}{r} N=3086379 \\ +\quad 18 \\ \hline +\ 308655 \\ 10 \\ \hline +\ 30875 \\ 10 \\ \hline +\ 3097 \\ 14 \\ \hline +\ 323 \\ 6 \\ \hline 38 \vdots 19,\ N \vdots 19. \end{array}$$

54. Если $6n+1=p_1-p_2$, то: а) из $p_2=2$ следует $p_1=6n+3$, что невозможно; б) из $p_2=2k+1$ следует $p_1=6n+2k+2$, что также невозможно.

55. Одно из простых чисел должно быть четным, поэтому имеем: $N=p-2$, где p — нечетное простое число.

56. Если $N^2=n^2+p$, то $p=(N-n)(N+n)$, откуда

$$\begin{cases} N-n=1, \\ N+n=p \end{cases}$$

и, следовательно, $2N=1+p$ или $p=2N-1=6m+3$, что невозможно.

57. Первый способ. Пусть $a=pq$, где p — наименьший простой делитель a. Если $p>\sqrt{a}$, то тем более $q>\sqrt{a}$ и, следовательно, $pq>a$, что противоречит условию. Значит, $p\leqslant\sqrt{a}$.

Второй способ. Из $p\leqslant q$ следует, что $ap\leqslant aq$, $p^2q<aq$ и $p^2\leqslant a$, $p\leqslant\sqrt{a}$.

Третий способ. Из $p\leqslant q$ следует $p^2\leqslant pq=a$ или $p<\sqrt{a}$. В случае простого a его наименьший простой делитель равен самому числу и теорема не верна.

58. 1) Простое, так как простые числа 2, 3, 5, 7, 11, не превышающие $\sqrt{127}$, не являются делителями 127. 2) Простое. 3) $7429=17\cdot19\cdot23$.

59. 1) Так как $\sqrt{109}=10,\ldots$, то наименьший простой делитель указанных чисел $\leqslant7$. Выпишем указанные числа и подчеркнем кратные 2, 3, 5 и 7:

101, $\underline{102}$, 103, $\underline{104}$, $\underline{105}$, $\underline{106}$, 107, $\underline{108}$, 109.

Так как $101=7\cdot14+3$, то наименьшее кратное семи число — четвертое от 101, т. е. 105; оно уже подчеркнуто, а следующее кратное семи число больше 109 (седьмое от 105). Следовательно, среди указанных чисел кратных 7 нет. Ответ: 101, 103, 107 и 109

2) 191, 193, 197 и 199. 3) 201 и 211.

60. Пусть p — простой делитель $n!-1$. Так как $p\leqslant n!-1$, то $p<n!$. С другой стороны, $n!$ не $\vdots\ p$, откуда $n<p$. Итак, $n<p<n!$.

Замечание. Из доказанного следует, что простых чисел бесконечное множество.

61. $13!+2$, $13!+3$, $\ldots$, $13!+13$.

62. Множество всех натуральных чисел по модулю 4 может быть разбито на 4 подмножества (по числу возможных остатков): на числа вида $4n$, $4n+1$, $4n+2$ и $4n+3$ ($n=0, 1, 2, \ldots$). Числа вида $4n$ и вида $4n+2$ составные. Следовательно, все простые числа содержатся среди натуральных чисел вида $4n+1$ и вида $4n+3$ (каждое из этих подмножеств действительно содержит простые числа, в чем легко убедиться).

63. При $n=2$ числа $n+10$ и $n+14$ являются составными. Натуральные числа $n\geqslant3$ можно записать в виде $n=3q+r$ $(0\leqslant r\leqslant2)$. При $r=2$ составным является число $n+10$, а при $r=1$ — число $n+14$. При $r=0$ имеем единственное простое число $n=3$, которому соответствуют простые числа $n+10=13$ и $n+14=17$. Ответ: $n=3$.

64. Для решения задачи целесообразно множество всех простых чисел разбить на 3 класса: класс простых чисел вида $3q$ $(q=1)$, класс простых чисел вида $3q+1$ $(q=2, 4, \ldots)$ и класс простых чисел вида $3q+2$ $(q=1, 3, \ldots)$. Единственное простое число первого класса $p=3$ удовлетворяет требованию задачи: $2\cdot 9+1=19$ — число простое. При $p=3q+1$ или $p=3q+2$ число $2p^2+1$ является составным — кратным трем. Ответ: $p=3$.

65. $p=5$. Исследовать классы простых чисел по модулю 5.

66. 1) Если $p=2$, то $p+10$ — число составное. Если $p=2q+1$ $(q=1, 2, \ldots)$, то число $p+5$ — составное. 3) Имеем либо $2^n=3q+1$, либо $2^n=3q+2$. В первом случае $2^n-1=3q$ — число составное, так как при $n>2$ имеем $q>1$. Во втором случае $2^n+1=3q+3$ — число составное.

67. Если $p=3k+1$ или $p=3k+2$, то число $8p^2+1$ составное (проверить!), поэтому следует рассмотреть $p=3$. При $p=3$ имеем $8p^2+1=73$ и $8p^2+2p+1=79$.

68. Рассмотрим числа p, $p+2$ и $p+4$ $(p>3)$. Положим $p=3q+1$ $(q=2, 4, \ldots)$, тогда $p+2$ — число составное (кратное 3). Если $p=3q+2$ $(q=1, 3, \ldots)$, то составным является число $p+4$.

70. Рассмотрим число $N=3\cdot 5\cdot 7\cdot \ldots \cdot p+2$, где p — простое число вида $3n+2$ (само число N также есть число вида $3n+2$). Каноническое разложение N содержит простые числа, большие p. Среди них непременно должно встретиться простое число вида $3n+2$, так как произведение простых чисел вида $3n+1$ есть число такого же вида и, следовательно, не может быть равно N. Итак, каково бы ни было p, существует число простое вида $3n+2$, большее p.

71. Члены данной прогрессии имеют вид $4n+3$ $(n=1, 2, \ldots)$. Каноническое разложение числа $N=4\cdot 5\cdot 7\cdot 11\cdot \ldots \cdot p+3$, где p — простое число вида $4n+3$, непременно содержит простое число вида $4n+3$, большее p (доказать!).

72. Пусть p — наибольшее простое число, удовлетворяющее условию $p\leqslant n$. Каноническое разложение $N=2\cdot 3\cdot 5 \ldots p-1$ содержит только простые числа, большие n. Следовательно, $N>n$, откуда тем более $2\cdot 3\cdot 5\cdot \ldots \cdot p>n$.

73. $\prod\limits_{i=1}^{n} p_i-1=p_k\cdot q$ $(k>n,\ q\geqslant 1)$, откуда $p_k\leqslant \prod\limits_{i=1}^{n} p_i-1$ и $p_k<\prod\limits_{i=1}^{n} p_i$. Тем более $P_{n+1}<\prod\limits_{i=1}^{n} p_i$.

74. $p_1=2^{2^0}$. Остается доказать, что $p_n\leqslant 2^{2^{n-1}}$ $(n=2, 3, \ldots)$. $p_2=3<2^{2^1}$; если $p_i<2^{2^{i-1}}$ $(i=2, 3, \ldots, n)$, то $p_{n+1}\leqslant \prod\limits_{k=1}^{n} p_k+1\leqslant$

$$\leqslant 2\cdot 2^2\cdot 2^{2^2}\ldots 2^{2^{n-1}}+1=2^{2^n-1}+1=2^{2^n}-2^{2^n-1}+1<2^{2^n}.$$

75. $p_5=11>10$. Если $p_n>2n$ $(n=5, 6, 7, \ldots, n)$, то из $p_{n+1}-p_n\geqslant 2$ следует $p_{n+1}-2n>2$ или $p_{n+1}>2(n+1)$.

Замечание. Объединяя результаты, полученные при решении задач 74 и 75, можно утверждать, что $2n<p_n<2^{2^{n-1}}$ $(n=5, 6, 7, \ldots)$.

76. По модулю 1.

79. $858-210=648 \vdots 12$. Но $385-77=308 \not\equiv 0 \pmod 6$, поэтому в данном случае требуется дополнительное исследование при помощи канонического разложения или алгоритма Евклида.

80. Первые два сравнения являются верными, остальные — неверными.

81. Доказать, что в каждом данном сравнении разность частей делится на модуль.

82. Доказать, что сравниваемые числа имеют с модулем различный НОД.

83. Если $a=mq+r$, то $a-r=mq$ и $a\equiv r \pmod m$.

84. $x=2+10q$ ($q=0, \pm 1, \pm 2, \ldots$).

85. 1) $x=3q$; 2) $x=1+2q$.

86. Найти натуральные делители разности данных чисел.

87. Натуральные делители разности $13-5$.

88. Пусть
$$\left.\begin{aligned} x&\equiv\alpha\\ y&\equiv\beta\\ z&\equiv\gamma\end{aligned}\right\} \pmod m,$$

тогда
$$\left.\begin{aligned} ax^3&\equiv a\alpha^3\\ bx^2y&\equiv b\alpha^2\beta\\ cxyz&\equiv c\alpha\beta\gamma\\ dz&\equiv d\gamma\end{aligned}\right\} \pmod m,$$

откуда $F(x, y, z)\equiv F(\alpha, \beta, \gamma) \pmod m$.

89. Использовать сравнение $3^4\equiv 1 \pmod{10}$.

90. Использовать сравнение $2^5\equiv 1 \pmod{31}$.

91. При $x=3n+1$ делимое равно $1+3\cdot 27^n+9\cdot 729^n$. По данному модулю $27^n\equiv 729^n\equiv 1$, поэтому $1+3\cdot 27^n+9\cdot 729^n\equiv 1+3+9=13$.

92. В разложении левой части сравнения по формуле Ньютона все биномиальные коэффициенты, кроме 1, кратны модулю.

Замечание. Ниже приводится доказательство обобщения данной теоремы при помощи теоремы Эйлера (задача 169).

93. По условию $a=b+p^nq$ ($q=0, \pm 1, \pm 2, \ldots$). Возводя части этого равенства в степень p, получаем $a^p=b^p+p^{n+1}\cdot\alpha$ ($\alpha=0, \pm 1, \pm 2, \ldots$).

94. Рассмотреть сравнения $a\alpha\equiv b\beta \pmod m$ и $\alpha\equiv\beta \pmod m$, где $(\alpha, m)=(\beta, m)=1$. Из второго сравнения $\alpha=\beta+mq$, поэтому первое сравнение можно записать в виде $a(\beta+mq)\equiv b\beta \pmod m$, откуда легко получить $a\equiv b \pmod m$.

96. Из левой части сравнения $a_4\cdot 10^4+\overline{a_3a_2}\cdot 10^2+\overline{a_1a_0}\equiv 0 \pmod{33}$ вычесть число $9999\cdot a_4+99\cdot\overline{a_3a_2}$, кратное модулю.

97. 1) Почленное перемножение указанных сравнений дает $\prod\limits_{i=1}^{n}(p-i)\equiv(-1)^n n! \pmod p$. Так как $(n!, p)=1$, то части полученного сравнения можно разделить на $n!$. 2) Имеем $\prod\limits_{i=2}^{n+1}(p-i)\equiv$ $\equiv(-1)^n(n+1)! \pmod p$, откуда $C_{p-2}^{n}\equiv(-1)^n\cdot(n+1) \pmod p$.

98. 1) Так как $9^{10}\equiv 1 \pmod{100}$, то $9^{10q+r}\equiv 9^r \pmod{100}$. Так как $9^9\equiv 9 \pmod{10}$, то $9^{9^9}\equiv 9^9\equiv 89 \pmod{100}$. Искомыми цифрами являются 8 и 9. 2) Так как $7^4=2401\equiv 1 \pmod{100}$, то и $7^{100}\equiv 1 \pmod{100}$, откуда $7^{9^{99}}\equiv 7^{100q+89}\equiv 7^{89} \pmod{100}$. Так как $7^{88}\equiv 1 \pmod{100}$, то $7^{89}\equiv 7 \pmod{100}$. Искомыми цифрами являются 0 и 7.

99. Из $p\equiv p+2\equiv 1 \pmod 2$ следует $p^{p+2}+(p+2)^p\equiv 0 \pmod 2$, а из

$$\left.\begin{aligned} p &\equiv -1 \\ p+2 &\equiv 1 \end{aligned}\right\} \pmod{p+1}$$

следует $p^{p+2}+(p+2)^p\equiv 0 \pmod{p+1}$.

100. За исключением нуля даны числа вида $\pm\frac{p-x}{2}$ $(x=1, 2, \ldots, \ldots, p-2)$. Сравнения

$$\left.\begin{aligned} \pm\frac{p-x}{2} &\equiv 0 \\ \frac{p-x_1}{2} &\equiv \pm\frac{p-x_2}{2} \end{aligned}\right\} \pmod p$$

приводят соответственно к неверным сравнениям

$$\left.\begin{aligned} x &\equiv p \\ x_1 &\equiv \pm x_2 \end{aligned}\right\} \pmod p.$$

101. Возводя в степень n и затем складывая

$$\left.\begin{aligned} 1 &\equiv 1-m \\ 2 &\equiv 2-m \\ &\ldots\ldots\ldots \\ m-2 &\equiv (m-2)-m=-2 \\ m-1 &\equiv (m-1)-m=-1 \\ m &\equiv -m \end{aligned}\right\} \pmod m,$$

получаем $\sum_{i=1}^{m} i^n\equiv\sum_{i=1}^{m}(-i)^n \pmod m$, откуда $2\sum_{i=1}^{m} i^n\equiv 0 \pmod m$ и $\sum_{i=1}^{m} i^n\equiv 0 \pmod m$.

102. При $n=1$ имеем верное сравнение. Если для некоторого n исходное сравнение верно, то оно верно и для $n+1$. Действительно, $2^{3^{n+1}}+1=(2^{3^n})^3+1=(2^{3^n}+1)(2^{2\cdot 3^n}-2^{3^n}+1)\equiv 0 \pmod{3^{n+2}}$, так как $2^{3^n}+1\equiv 0 \pmod{3^{n+1}}$ по допущению и $2^{2\cdot 3^n}-2^{3^n}+1\equiv \pmod 3$ в силу того, что $2\equiv -1 \pmod 3$.

103. Так как $2^{3^n}+1\equiv 0 \pmod{3^{n+1}}$, то тем более $2^{3^n}+1\equiv 0 \pmod{3^n}$, откуда $2^m+1\equiv 0 \pmod m$, где $m=3^n$.

104. При $n=1$ данное сравнение имеет вид $(m-1)^m \equiv \equiv -1 \pmod{m^2}$ или $(m-1)^m+1=m[(m-1)^{m-1}-(m-1)^{m-2}+\ldots \ldots+1]\equiv 0 \pmod{m^2}$, откуда $(m-1)^{m-1}-(m-1)^{m-2}+\ldots+1\equiv \equiv 0 \pmod{m}$, $(-1)^{m-1}-(-1)^{m-2}+\ldots+1\equiv 0 \pmod{m}$ или $\underbrace{1+1+\ldots+1}_{m \text{ слагаемых}}\equiv 0 \pmod{m}$. Последнее сравнение верно и равносильно исходному, следовательно, данное сравнение верно при $n=1$. Если данное сравнение верно для некоторого n, то $(m-1)^{m^{n+1}}+1= =[(m-1)^{m^n}]^m+1=[(m-1)^{m^n}+1][(m-1)^{(m-1)m^n}- -(m-1)^{(m-2)m^n}+\ldots+1]\equiv 0 \pmod{m^{n+2}}$, так как $(m-1)^{m^n}+1\equiv \equiv 0 \pmod{m^{n+1}}$ по допущению и $(m-1)^{(m-1)m^n}-(m-1)^{(m-2)m^n}+ +\ldots+1\equiv 0 \pmod{m}$ в силу сравнения $m-1\equiv -1 \pmod{m}$ и нечетности m.

105. При $m=5$ сравнение $(m-1)^{m^n}\equiv -1 \pmod{m^{n+1}}$ принимает вид $4^{5^n}+1\equiv 0 \pmod{5^{n+1}}$, откуда $4^{5^n}+1\equiv 0 \pmod{5^n}$. Таким образом, имеем $2^{2x}+1\equiv 0 \pmod{x}$, где $x=5^n$ $(n=1, 2, 3, \ldots)$.

106. 1) $2^{4n+1}=2\cdot 4^{2n}\equiv 2 \pmod 5$, так как $4\equiv -1 \pmod 5$. Таким образом, $2^{4n+1}=2+5k$, где k — число натуральное, и $N=3^{2+5k}+ +2=9\cdot 243^k+2\equiv 0 \pmod{11}$, так как $243\equiv 1 \pmod{11}$. Итак, $N \vdots 11$ и $N>11$. Следовательно, N — число составное. 2) $3^{4n+1}=3\cdot 9^{2n}\equiv \equiv 3 \pmod{10}$, так как $9\equiv -1 \pmod{10}$. Значит, $3^{4n+1}=3+10k$, где k — число натуральное, и $M=2^{3+10k}+3=8\cdot 32^{2k}+3\equiv 0 \pmod{11}$, так как $32\equiv -1 \pmod{11}$. Из того, что $M>11$ и $M \vdots 11$, следует, что M — число составное.

107. 1) $19^z\equiv 1 \pmod 3$, так как $19\equiv 1 \pmod 3$. Но $2^x+7^y\equiv \equiv(-1)^x+1 \pmod 3$, откуда в зависимости от четности x либо $2^x+7^y\equiv 2 \pmod 3$, либо $2^x+7^y\equiv 0 \pmod 3$. Таким образом, $2^x+7^y\not\equiv 19^z \pmod 3$, откуда $2^x+7^y\neq 19^z$ (если x, y и z — натуральные числа). 2) $2^x+5^y\equiv(-1)^x+(-1)^y \pmod 3$ и, следовательно, при нечетных значениях x и y имеем $2^x+5^y\equiv -2\equiv 1 \pmod 3$, откуда $2^x+5^y\equiv 19^z \pmod 3$. Однако если при некоторых натуральных значениях x, y и z имеет место равенство $2^x+5^y=19^z$, то при этих значениях переменных 2^x+5^y и 19^z должны быть сравнимы по любому модулю. Между тем если при $x=2n+1$ и $y=2n+1$ имеем $2^x+5^y= =4^n\cdot 2+5^{2n+1}\equiv(-1)^n\cdot 2 \pmod 5$, то $19^z\equiv(-1)^z \pmod 5$, откуда видно, что $2^{2n+1}+5^{2n+1}\not\equiv 19^z \pmod 5$. Значит, $2^x+5^y\neq 19^z$, где x, y и z — натуральные числа.

Замечание. Конечно, неразрешимость данных уравнений в натуральных числах можно доказать и без применения сравнений. Например, относительно первого уравнения имеем $2^x=19^z-7^y= =(19^z-1)-(7^y-1)=18(19^{z-1}+19^{z-2}+\ldots+1)-6(7^{y-1}+7^{y-2}+ +\ldots+1)$, откуда видно, что $(19^z-7^y) \vdots 3$, тогда как 2^x не $\vdots 3$.

108. По условию $11a+2b\equiv 0 \pmod{19}$ или $30a+2b\equiv 0 \pmod{19}$, откуда $b\equiv 4a \pmod{19}$. Таким образом, $18a+5b\equiv 18a+20a=38a\equiv \equiv 0 \pmod{19}$, т. е. $\dfrac{18a+5b}{19}$ — число целое.

109. $x\equiv 0;\ 1;\ 2;\ \ldots;\ 9 \pmod{10}$.

111. 1) $x\equiv 1;\ 3;\ 7;\ 9 \pmod{10}$. 2) $x\equiv 2;\ 4;\ 6;\ 8 \pmod{10}$. 3) $x\equiv 5 \pmod{10}$. 4) $x\equiv 0 \pmod{10}$.

112. Во-первых, число классов по модулю md в d раз больше числа классов по модулю m. Во-вторых, числа, не сравнимые по модулю m, не сравнимы и по модулю md.

115. Так как по модулю 5 данные числа сравнимы соответственно с 0, 1, 2, 3, 4, то искомый модуль равен 5.

116. Попытаться установить соответствие между данными числами и остатками по модулю 10.

117. Записать данные числа в виде $a+x$ $(x=0, 1, 2, \ldots, m-1)$, где a — произвольное целое число, и применить теорему о вычетах линейной формы.

118. Убедиться в том, что дано m чисел, не сравнимых по модулю m.

119. Можно воспользоваться значениями x, составляющими полную систему остатков по модулю 10.

121. $x_{i_1} \equiv x_{i_2} \pmod m$ приводит к $ax_{i_2}+b \equiv ax_{i_1}+b \pmod m$, что противоречит условию.

123. Рассмотреть соответствующие остатки по модулю 7.

130. Из условия $(a, m)=d$ следует $\left(\frac{a}{d}, \frac{m}{d}\right)=1$.

132. См. рисунок 1.

133. 1) 400; 2) 100; 3) 48; 4) 96; 5) 720.

134. $\varphi(1225)=840$.

135. $\varphi(m)$.

136. $120-\varphi(120)=88$.

137. Каждому классу $x \equiv a \pmod m$, где $(a, m)=d$, взаимно и однозначно соответствует класс $\frac{x}{d} \equiv \frac{a}{d} \left(\mathrm{mod}\ \frac{m}{d}\right)$, где $\left(\frac{a}{d}, \frac{m}{d}\right)=1$. Но число классов второго типа равно $\varphi\left(\frac{m}{d}\right)$.

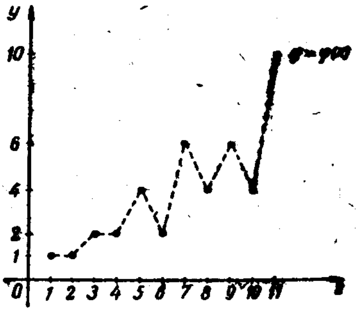

Рис. 1

138. 3) Пусть $m=\prod_{i=1}^{k} p_i^{\alpha_i}$. Тогда $\varphi(m^\alpha)=m^\alpha \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)=$
$=m^{\alpha-1}\left[m\prod_{i=1}^{k}\left(1-\frac{1}{p}\right)\right]=m^{\alpha-1}\varphi(m)$.

139. Первый случай имеет место при $(m, 2)=1$, второй — в противном случае, т. е. при $(m, 2)=2$.

140. 1) $\varphi(4n+2)=\varphi(2)\,\varphi(2n+1)=\varphi(2n+1)$. 2) Если $(n, 2)=1$, то $\varphi(4n)=\varphi(4)\varphi(n)=2\varphi(n)$. Если же $n=2^\alpha\cdot k$, где $(k, 2)=1$, то $\varphi(4n)=\varphi(2^{\alpha+2}\cdot k)=2^{\alpha+1}\cdot\varphi(k)=2\cdot\varphi(2^{\alpha+1}\cdot k)=2\varphi(2n)$.

141. 1) $5^{x-1}\cdot 4=100$, $x=3$. 2) $x=3$. 3) $p^{x-1}\cdot(p-1)=p^{x-1}$. Это уравнение не имеет решения при $p>2$. При $p=2$ ему удовлетворяет любое натуральное значение неизвестного. 4) $3^{x-1}\cdot 5^{y-1}\cdot 2\cdot 4=600$, $3^{x-1}\cdot 5^{y-1}=3\cdot 5^2$, $x=2$ и $y=3$.

142. Из формулы $\varphi(m)=\prod\limits_{i=1}^{k} p_i^{\alpha_i-1}\cdot\prod\limits_{i=1}^{k}(p_i-1)$, где $m=\prod\limits_{i=1}^{k} p_i^{\alpha_i}$, видно, что каждому нечетному p_i соответствует четный множитель p_i-1 и, следовательно, четное значение $\varphi(m)$. Если же $m=2^\alpha>3$, то четность $\varphi(m)$ очевидна.

143. Если $(m, 2)=1$, то $\varphi(m)=\varphi(2m)$.

144. Каждому простому числу p, являющемуся делителем как m, так и n, соответствует в числе $\varphi(mn)$ множитель $1-\frac{1}{p}$, а в числе $\varphi(m)\varphi(n)$ — множитель $\left(1-\frac{1}{p}\right)^2$. Так как $1-\frac{1}{p}<1$, то при данном условии $\varphi(m)\varphi(n)<\varphi(mn)$. В частности, $\varphi^2(m)\leqslant\varphi(m^2)$, причем равенство имеет место только при $m=1$.

145. Пусть $q_1, q_2, \ldots, q_t$ — простые числа, входящие в каноническое разложение только m, $p_1, p_2, \ldots, p_k$ — простые числа, входящие в каноническое разложение как m, так и n, и $l_1, l_2, \ldots, l_s$ — простые числа, входящие в каноническое разложение только n. Тогда

$$\varphi(mn)=mn\prod_{i=1}^{t}\left(1-\frac{1}{q_i}\right)\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\cdot\prod_{i=1}^{s}\left(1-\frac{1}{l_i}\right)=$$

$$=\left[m\prod_{i=1}^{t}\left(1-\frac{1}{q_i}\right)\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\right]\cdot\left[n\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\times\right.$$

$$\left.\times\prod_{i=1}^{s}\left(1-\frac{1}{l_i}\right)\right]\cdot\frac{d}{d\cdot\prod\limits_{i=1}^{k}\left(1-\frac{1}{p_i}\right)}=\varphi(m)\varphi(n)\cdot\frac{d}{\varphi(d)}.$$

Замечание 1. При помощи выведенной формулы задача 144 решается автоматически: $\varphi(m)\varphi(n)\leqslant\varphi(mn)$, так как $\frac{d}{\varphi(d)}\geqslant 1$, причем равенство имеет место тогда и только тогда, когда $d=1$.

Замечание 2. Аналогично может быть выведено соотношение $\varphi(mn)=\varphi(m)\varphi(n)\cdot\frac{A}{\varphi(A)}$, где A — произведение общих делителей m и n.

146. $\varphi(mn)=\varphi(\delta\mu)=\varphi(\delta)\varphi(\mu)\cdot\frac{\delta}{\varphi(\delta)}=\delta\varphi(\mu)$.

147. Данную сумму можно представить в виде $1+(p-1)+(p^2-p)+\ldots+(p^{\alpha-1}-p^{\alpha-2})+(p^\alpha-p^{\alpha-1})$, откуда видно, что она равна p^α.

148. Каждое слагаемое выражает число классов, имеющих с модулем m НОД d_i ($i=1, 2, \ldots, k$) (см. задачу 137). Следовательно, данная сумма выражает общее число классов по модулю m и равна m.

149. Каждому делителю d_i соответствует делитель $\frac{m}{d_i}$, поэтому $\Sigma\varphi(d_i)$ выражает то же, что и $\Sigma\varphi\left(\frac{m}{d_i}\right)$.

Замечание. Задача 147 является частной относительно задачи 149 (или 148): числа p^x ($x=0, 1, 2, \ldots, \alpha$) исчерпывают все натуральные делители модуля p^{α}.

150. Всего таких чисел $\varphi(m)$. Каждому натуральному числу x, удовлетворяющему условиям $x \leqslant m$ и $(x, m)=1$, соответствует число $m-x$, удовлетворяющее тем же условиям. Сумма каждой пары таких чисел равна m. Таких пар $\frac{1}{2}\varphi(m)$, поэтому их общая сумма равна $\frac{1}{2}m\varphi(m)$.

151. Воспользоваться результатом задачи 150.

152. Необходимо, чтобы $\varphi(m)=2$. Но $1\equiv 5 \pmod 4$, поэтому ответом служат только числа 3 и 6.

153. Необходимо и достаточно, чтобы $\varphi(m)=4$. Из формулы Гаусса следует, что модуль m надо искать среди чисел вида 2^x либо $2^x\cdot 3$, либо $2^x\cdot 5$. Исследование этих возможностей дает: $m=8$; 12; 5; 10.

154. 1) Из формулы Гаусса следует, что $x=2^y\cdot 3^z\cdot 5^u$ ($y\geqslant 0$, $z=0$; 1, $u=0$; 1). Исследование возможностей $x=2^y$; $2^y\cdot 3$; $2^y\cdot 5$; $2^y\cdot 15$; 3; 5; 15 дает: $x=2^{\alpha+1}$; $2^{\alpha}\cdot 3$; $2^{\alpha-1}\cdot 5$; $2^{\alpha-2}\cdot 15(\alpha\geqslant 2)$; $15(\alpha=3)$. 2) При $p\neq 3$ решений нет. При $p=3$ уравнению удовлетворяет любое целое $x\geqslant 2$.

155. 1) Положив $x=p^{\alpha}\cdot y$, где $(y, p)=1$, имеем $p^{\alpha-1}\varphi(y)=1$, откуда $\alpha=1$ и $\varphi(y)=1$. Следовательно, при $p=2$ уравнение имеет единственное решение $x=2$ (так как в этом случае $y=1$); при $p>2$ уравнение имеет два решения: $x=p$; $2p$. 2) Необходимо, чтобы $\varphi(x) \vdots 7$, т. е. чтобы каноническое разложение x содержало число 7. Но в этом случае $\varphi(x) \vdots 6$, что противоречит условию $\varphi(x)=14$. Уравнение не имеет решений. 3) $x=16$; 24; 20; 30; 15 (см. уравнение 1 задачи 154). 4) $x=36$; 28; 13; 26; 21; 42.

156. $3^{\alpha-1}\cdot 5^{\beta-1}\cdot 7^{\gamma-1}\cdot 2\cdot 4\cdot 6=3600$ или $3^{\alpha}\cdot 5^{\beta-1}\cdot 7^{\gamma-1}=3^2\cdot 5^2$, откуда $\alpha=2$, $\beta=3$, $\gamma=1$ и $m=7875$.

157. $(p_1-1)(p_2-1)=120$ и $p_1-p_2=2$, откуда $p_1=13$, $p_2=11$ и $x=143$.

158. $m=14161$. Представляя уравнение в виде $p_1p_2(p_1-1)(p_2-1)=2^5\cdot 3\cdot 7\cdot 17$, исследовать гипотезы: $p_1=2$; 3; 7; 17.

159. 1) При $p=2$ уравнению удовлетворяет любое нечетное значение неизвестного, а при $p>2$ — решений нет. Исследовать случаи $(x, p)=1$ и $(x, p)=(p, 2)$ x — натуральное число, кратное p. 3) При $p_1=2$ и $p_2=3$ (или наоборот) уравнению удовлетворяет любое число вида $2^{\alpha}\cdot q$, где $(q, 2)=(q, 3)=1$.

160. 1) По условию $x=2^{\alpha}\cdot q$, где $(q, 2)=1$ и α — число натуральное. Уравнение принимает вид $2^{\alpha-1}\cdot\varphi(q)=2^{\alpha-1}\cdot q$, откуда $q=1$ и $x=2^{\alpha}$. 2) $x=2^{\alpha_1}\cdot 3^{\alpha_2}$, $\alpha_1\geqslant 1$, $\alpha_2\geqslant 1$. 3) Решений нет.

Замечание. Полезно рассмотреть графическое решение данных уравнений.

161. $x=1+\dfrac{\ln\dfrac{a}{p-1}}{\ln p}$, где параметр a либо 1, либо число четное.

162. Если p_i $(i=1, 2, \ldots, k)$ — все простые числа, то для $a=\prod_{i=1}^{k} p_i$ имеем $\varphi(a)=\prod_{i=1}^{k}(p_i-1)$. С другой стороны, $\varphi(a)=1$, так как любое натуральное число, не превышающее a и отличное от 1, имеет простой делитель, равный одному из чисел p_i, и, следовательно, не является взаимно простым с a. Итак, $\prod_{i=1}^{k}(p_i-1)=1$, что невозможно, так как уже при $k=2$ имеем $(2-1)(3-1)>1$. Полученное противоречие и доказывает бесконечность множества всех простых чисел.

163. Пусть $m=\prod_{i=1}^{k} p_i^{\alpha_i}$. Требуется из общего числа m^n размещений вычесть число размещений, компоненты которых кратны p_i. Так как $\dfrac{m}{p_1}$ числам, не превышающим m и кратным p_1, соответствует $\left(\dfrac{m}{p_1}\right)^n$ размещений по n таких чисел, то существует

$$m^n-\left(\frac{m}{p_1}\right)^n=m^n\left(1-\frac{1}{p_1^n}\right)$$

размещений, состоящих из чисел, взаимно простых с p_1. Так как из $\left(\dfrac{m}{p_2}\right)^n$ размещений, компоненты которых кратны p_2, уже учтено $\left(\dfrac{m}{p_1p_2}\right)^n$ размещений, то остается учесть

$$\left(\frac{m}{p_2}\right)^n-\left(\frac{m}{p_1p_2}\right)^n=\left(\frac{m}{p_2}\right)^n\left(1-\frac{1}{p_1^n}\right).$$

Таким образом, размещений, состоящих из n чисел, взаимно простых с p_1 и p_2, существует

$$m^n\left(1-\frac{1}{p_1^n}\right)-\left(\frac{m}{p_2}\right)^n\left(1-\frac{1}{p_1^n}\right)=m^n\left(1-\frac{1}{p_1^n}\right)\left(1-\frac{1}{p_2^n}\right).$$

Методом математической индукции можно доказать, что

$$\varphi_n(m)=m^n\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i^n}\right),$$

где $\varphi_n(m)$ — число размещений с повторениями из m первых натуральных чисел по n таких, НОД которых взаимно прост с m.

Замечание. Обобщенная функция Эйлера $\varphi_n(m)$ мультипликативна, для нее имеет место равенство $\sum_{i=1}^{t}\varphi_n(d_i)=m^n$, где d_i — все возможные делители m.

164. По условию $x^4 \equiv 1 \pmod{10}$, откуда $x^{12} \equiv 1 \pmod{10}$.

165. $a^{p-1} \equiv 1 \pmod{p}$, откуда $a^{p-1}+p-1 \equiv p \equiv 0 \pmod{p}$.

166. Имеем $a^{12} \equiv b^{12} \equiv 1 \pmod{13}$ и $a^4 \equiv b^4 \equiv 1 \pmod{5}$, откуда $a^{12} \equiv b^{12} \equiv 1 \pmod{5}$; следовательно, $a^{12} \equiv b^{12} \equiv 1 \pmod{65}$ или $a^{12}-b^{12} \vdots 65$.

167. Сложить почленно сравнения $i^{k(p-1)} \equiv 1 \pmod{p}$, где $i = 1, 2, \ldots, p-1$.

168. $2^{11} \equiv 2 \pmod{11}$, откуда $2^{11\cdot 31} \equiv 2^{32} = 2\cdot 64^5 \equiv 2\cdot(-2)^5 = -64 \equiv 2 \pmod{11}$; $2^{31} \equiv 2 \pmod{31}$, откуда $2^{11\cdot 31} \equiv 2^{11} = 64\cdot 32 \equiv 2 \pmod{31}$.

169. Использовать сравнение $a^p \equiv a \pmod{p}$.

170. Данное сравнение является обобщением сравнения $a^p \equiv a \pmod{p}$ и доказывается аналогично.

171. Пусть $\varphi(m) = P_m(a)\cdot q + r$, где $q \geqslant 0$ и $0 \leqslant r < P_m(a)-1$. Из $a^{P_m(a)} \equiv 1 \pmod{m}$ следует $a^{\varphi(m)} \equiv a^r \equiv 1 \pmod{m}$, откуда $r=0$.

172. Применить теорему предыдущей задачи.

173. Если $(x, p) = 1$, то $x^{(p-1)m}+x^{(p-1)n} \equiv 2 \pmod{p}$.

174. Так как $(m, 10) = 1$, то $10^{\varphi(m)} \equiv 1 \pmod{m}$ или $10^{\varphi(m)}-1 = 99\ldots9 \equiv 0 \pmod{m}$. Так как $(9, m) = 1$, то части полученного сравнения можно разделить на 9.

175. 1) $561 = 3\cdot 11\cdot 17$. По условию $(a, 3) = 1$, поэтому $a^2 \equiv 1 \pmod{3}$, откуда $a^{560} \equiv 1 \pmod{3}$. Аналогично могут быть получены сравнения $a^{560} \equiv 1$ (mod 11 и 17). Теперь справедливость данной теоремы очевидна. 2) Число 1093 простое, поэтому $\varphi(1093^2) = 1093\cdot 1092$, и по теореме Эйлера $2^{1093\cdot 1092} \equiv 1 \pmod{1093^2}$.

176. 1) Имеем $x^7 \equiv x \pmod{7}$. Остается доказать, что $x^7 \equiv x$ (mod 2 и 3), для чего можно воспользоваться теоремой задачи 170 или просто испытать полную систему остатков по модулям 2 и 3. 2) $2730 = 2\cdot 3\cdot 5\cdot 7\cdot 13$. Имеем $x^{13} \equiv x \pmod{13}$. Справедливость сравнений $x^{13} \equiv x$ (mod 2, 3, 5 и 7) вытекает из сравнения задачи 170.

177. Если $(a, 5) = 1$, то $a^{\varphi(125)} = a^{100} \equiv 1 \pmod{125}$. Если же $(a, 5) = 5$, то $a^{100} \equiv 0 \pmod{125}$.

178. $a_i^5 \equiv a_i \pmod{30}$, так как $a_i^5 \equiv a_i$ (mod 2, 3, 5) (см. задачу 170). Таким образом, $\sum\limits_{i=1}^{n} a_i^5 \equiv \sum\limits_{i=1}^{n} a_i \equiv 0 \pmod{30}$.

179. Перемножить почленно $p_1^{p_2-1}-1 = p_2\cdot q_1$ и $p_2^{p_1-1}-1 = p_1\cdot q_2$, где q_1 и q_2 — числа целые.

180. Так как $(2p+1, 3) = 1$, то $(2p+1)^2 \equiv 1 \pmod{3}$, откуда $4p+1 \equiv 0 \pmod{3}$.

181. По условию $a^{\varphi(m)} \equiv 1 \pmod{m}$ и $\alpha_1 = \alpha_2+\varphi(m)\cdot q$. Следовательно, $a^{\alpha_2+\varphi(m)\cdot q} \equiv a^{\alpha_2} \pmod{m}$ или $a^{\alpha_1} \equiv a^{\alpha_2} \pmod{m}$.

182. Легко проверить, что $p \neq 5$. Таким образом, $5^{p-1} \equiv 1 \pmod{p}$, откуда $5^{p^2-1} \equiv 1 \pmod{p}$ и $5^{p^2}+1 \equiv 6 \pmod{6}$. Так как необходимо, чтобы $6 \equiv 0 \pmod{p}$, то значение p следует искать среди чисел 2 и 3. Проверка показывает, что $p=3$.

183. Пусть $2^{\varphi(m)-1} \equiv r \pmod{m}$, где $0 \leqslant r < m$. Тогда $2^{\varphi(m)} \equiv 2r \equiv 1 \pmod{m}$ или $r = \dfrac{1+mq}{2}$, где q — число целое. Условию $0 \leqslant r < m$

удовлетворяет единственное значение $\frac{1+mq}{2}$ при $q=1$, откуда $r=\frac{1+m}{2}$.

184. Из $a^{\varphi(m)}\equiv 1 \pmod m$ следует $a[-b\cdot a^{\varphi(m)-1}]+b\equiv 0 \pmod m$, откуда $x\equiv -b\cdot a^{\varphi(m)-1} \pmod m$.

185. 1) $x\equiv 2 \pmod 3$; 2) $x\equiv 1;\ 3 \pmod 4$; 3) $x\equiv 1;\ 3 \pmod 5$. Данное сравнение целесообразно представить в виде

$$2x^2+2x+1\equiv 0 \pmod 5.$$

188. Следует решить сравнение $5x^2+x+4\equiv 0 \pmod{10}$.

Первый способ. Необходимо, чтобы $5x^2+x+4\equiv 0 \pmod 2$ или $x(x+1)\equiv 0 \pmod 2$, откуда $x\equiv 0;\ 1 \pmod 2$ или $x=2q;\ 2q+1$. Подстановка $x=2q$ в исходное сравнение после обычных преобразований дает $q\equiv 3 \pmod 5$ или $q=3+5t$, откуда $x=6+10t$ или $x\equiv 6 \pmod{10}$. При $x=2q+1$ исходное сравнение дает $q\equiv 0 \pmod 5$ или $q=5t$, откуда $x=10t+1$ или $x\equiv 1 \pmod{10}$. Таким образом, данный трехчлен делится на 10 при $x\equiv 6;\ 1 \pmod{10}$.

Второй способ. Необходимо, чтобы $5x^2+x+4\equiv 0 \pmod 5$ или $x\equiv 1 \pmod 5$. По модулю 10 имеем два класса значений аргумента (задача 112): $x\equiv 1;\ 6 \pmod{10}$. Проверка показывает, что все эти значения неизвестного удовлетворяют исходному сравнению.

189. $x\equiv 1;\ 3 \pmod 6$. Для упражнения полезно решить данное сравнение, используя необходимое условие $x^2-4x+3\equiv 0 \pmod 3$.

190. По теореме Эйлера данное сравнение имеет $\varphi(30)=8$ решений: $x\equiv 1;\ 7;\ 11;\ 13;\ 17;\ 19;\ 23;\ 29 \pmod{30}$. При этом, конечно, учитывается, что верна теорема, обратная теореме Эйлера: если $a^{\varphi(m)}\equiv 1 \pmod m$, то $(a, m)=1$.

191. 1) $\varphi(m)$; 2) $x\equiv 1;\ 2;\ \ldots;\ p-1 \pmod p$.

192. Из условия следует, что $b_ix^{n-i}\equiv a_ix^{n-i} \pmod m$, откуда $\sum_{i=0}^{n} b_ix^{n-i}\equiv \sum_{i=0}^{n} a_ix^{n-i} \pmod m$. Полученное сравнение и доказывает равносильность сравнений $\sum_{i=0}^{n} b_ix^{n-i}\equiv 0 \pmod m$ и $\sum_{i=0}^{n} a_ix^{n-i}\equiv 0 \pmod m$.

193. Имеем $ax_0\equiv 1 \pmod m$, откуда $a\cdot bx_0\equiv b \pmod m$.

194. Общий вид искомых сравнений $x^2+bx+c\equiv 0 \pmod 2$. Дальнейшее исследование приводит к сравнению $x^2+x+1\equiv 0 \pmod 2$. Относительно модуля 3 задача имеет 3 решения:

$$\left.\begin{aligned} x^2+1&\equiv 0,\\ x^2+x+2&\equiv 0,\\ x^2+2x+2&\equiv 0 \end{aligned}\right\} \pmod 3.$$

195. Частное от деления $\Phi(x)$ на x^p-x есть некоторый полином $Q(x)$ с целыми коэффициентами, удовлетворяющий тождеству

$\Phi(x)=(x^p-x)\cdot Q(x)+R(x)$. Поэтому данное сравнение равносильно сравнению $(x^p-x)\cdot Q(x)+R(x)\equiv 0 \pmod p$. Остается учесть, что $x^p-x\equiv 0 \pmod p$.

196. 1) Остаток от деления левой части сравнения на x^3-x равен $x-1$, следовательно, данное сравнение равносильно сравнению $x-1\equiv 0 \pmod 3$, откуда $x\equiv 1 \pmod 3$. 2) Данное сравнение равносильно сравнению $-x^2\equiv 0 \pmod 5$, откуда $x\equiv 0 \pmod 5$. 3) Имеем $x^2-3x+2\equiv 0 \pmod 5$, откуда $x\equiv 1;\ 2 \pmod 5$. 4) $x\equiv 1 \pmod{11}$. 5) $x\equiv -1 \pmod{13}$.

197. $x^p\equiv x \pmod p$ следует $a_i x^{n-i}\equiv a_i x^{q_i+r_i} \pmod p$, где $i=0,\ 1,\ 2,\ \dots,\ k$, откуда $\sum\limits_{i=0}^{k} a_i x^{n-i}\equiv \sum\limits_{i=0}^{k} a_i x^{q_i+r_i} \pmod p$ и $\sum\limits_{i=0}^{n} a_i x^{n-i}\equiv \sum\limits_{i=0}^{k} a_i x^{q_i+r_i}+\sum\limits_{i=k+1}^{n} a_i x^{n-i}\equiv 0 \pmod p$.

198. 1) Имеем $x^4-x+1\equiv 0 \pmod 3$, откуда испытанием системы остатков находим $x\equiv 2 \pmod 3$. 2) Имеем $5x-3\equiv 0 \pmod 7$ или $-2x+4\equiv 0 \pmod 7$, откуда $x\equiv 2 \pmod 7$. 3) Имеем $x^4-x^3+1\equiv \equiv 0 \pmod 5$, откуда $x\equiv 3 \pmod 5$.

199. 1) $x\equiv 10 \pmod{17}$; 2) $x\equiv -3 \pmod{29}$; 3) $x\equiv 6 \pmod 9$; 4) $x\equiv 7 \pmod{10}$; 5) после прибавления к правой части $2ab$ имеем $(a+b)x\equiv (a+b)^2 \pmod{ab}$, откуда $x\equiv a+b \pmod{ab}$; 6) имеем: $(a-b)^2x\equiv a-b \pmod{ab}$ или $(a-b)x\equiv 1 \pmod{ab}$, откуда $x\equiv \equiv (a-b)^{\varphi(ab)-1} \pmod{ab}$; 7) имеем $(a+b)x\equiv a-b \pmod{ab}$, откуда $x\equiv (a-b)\cdot(a+b)^{\varphi(ab)-1} \pmod{ab}$; 8) $2x\equiv 1+p \pmod p$, откуда $x\equiv \frac{1+p}{2} \pmod p$.

200. 1) $x\equiv 1;\ 6 \pmod{10}$; 2) $x\equiv 1;\ 4;\ 7;\ 10 \pmod{12}$; 3) решений нет; 4) $x\equiv 5;\ 12;\ 19;\ 24;\ 29 \pmod{35}$; 5) $x\equiv -1 \pmod m$; 6) $x\equiv a \pmod m$; 7) $x\equiv a^{p-2} \pmod p$; 8) если $(a+1,\ m)=1$, то $x\equiv a-1 \pmod m$; если же $(a+1,\ m)=d>1$, то имеем $\frac{a+1}{d}\,x\equiv \equiv \frac{a^2-1}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$, где $\left(\frac{a+1}{d},\ \frac{m}{d}\right)=1$, откуда $x\equiv a-1 \left(\mathrm{mod}\ \frac{m}{d}\right)$; по данному модулю имеем d решений: $x\equiv a-1;\ a-1+\frac{m}{d};\ a-1+\frac{2m}{d};\ \dots;\ a-1+\frac{(d-1)m}{d} \pmod m$.

201. Все указанные значения x записать по модулю 12.

202. 1) Из сравнения $5x\equiv 3 \pmod 4$ находим $x=3+4q$. Подставляя в данное уравнение, получаем $y=-3-5q$. 2) $x=-3+13q$, $y=4-17q$. 3) Имеем $13x-4y=5$, откуда $x=1+4q$, $y=2+13q$. 4) $x=2+3q$, $y=-2q$. 5) $x=2+3q$, $y=2+4q$.

203. Имеем $5a-9b=31$ или $5a\equiv 31 \pmod 9$. Наименьшее натуральное значение a, удовлетворяющее этому условию, есть $a=8$. Соответствующее значение b есть $b=1$.

204. Имеем $8x+6\equiv 0 \pmod{13}$, откуда $x=9+13t$. Условию $-100<9+13t<150$ удовлетворяет 19 значений t. Искомое число целых точек равно 19.

205. Имеем $7y\equiv-1 \pmod 3$, откуда $y=2+3t$. Условию $-1<2+3t<2$ не удовлетворяет ни одно целое значение t.

206. Из $ax+by=n$ следует $ax\equiv n \pmod b$, откуда $x=n\cdot a^{\varphi(b)-1}+bq$. Чтобы эти значения x были натуральными, надо, чтобы $q>-\frac{n\cdot a^{\varphi(b)}}{ab}$. Подставляя эти значения x в исходное уравнение,

имеем $y=\frac{n-n\cdot a^{\varphi(b)}-abq}{b}$. Чтобы эти значения y были натуральными, надо, чтобы $n-n\cdot a^{\varphi(b)}-abq>0$, т. е. $q<-\frac{n\cdot a^{\varphi(b)}}{ab}+\frac{n}{ab}$. Итак, исходное уравнение имеет натуральное решение при целых значениях q, удовлетворяющих условию

$$-\frac{n\cdot a^{\varphi(b)}}{ab}<q<-\frac{n\cdot a^{\varphi(b)}}{ab}+\frac{n}{ab}.$$

Такие значения q существуют, так как длина отрезка $\left[-\frac{n\cdot a^{\varphi(b)}}{ab}, -\frac{n\cdot a^{\varphi(b)}}{ab}+\frac{n}{ab}\right]$, равная $\frac{n}{ab}$, при $n>ab$ больше 1. Например, уравнение $3x+4y=13$, имеющее целочисленные решения $x=3+4q$, $y=1-3q$, при $q=0$ имеет решение в натуральных числах: $x=3$, $y=1$.

Если $ax+by=ab$, то $ax\equiv0 \pmod b$, откуда $x=bd, q=1, 2, 3, \ldots$. Подставляя эти значения x в исходное уравнение, получаем $y=a(1-q)\leqslant0$. Таким образом, число $n=ab$, где $(a, b)=1$, не может быть представлено в виде $ax+by$, где x и y — числа натуральные.

207. 1) $9x\equiv1 \pmod 7$, откуда $x=4+7q$. 2) $x=13+15q$.

208. Если $\frac{2n+1}{n(n+1)}=\frac{x}{n}+\frac{y}{n+1}$, где x и y — числа натуральные, то $(n+1)x+ny=2n+1$, откуда $(n+1)x\equiv2n+1 \pmod n$ и $x=1+nq$, $q=0, 1, 2, \ldots$. Подставляя эти значения x в уравнение, получаем $y=1-(n+1)q$, откуда находим единственное натуральное значение y при $q=0$. Итак, имеем единственное представление: $\frac{2n+1}{n(n+1)}=\frac{1}{n}+\frac{1}{n+1}$.

209. Следует найти двузначные числа x, удовлетворяющие сравнениям $3200+x\equiv0 \pmod{21}$ и $100x+32\equiv0 \pmod{21}$.

210. $60x+80y=440$, откуда $x=2$, $y=4$ и $x=6$, $y=1$.

211. $48-5q$ и $1+3q$, $q=0, 1, 2, \ldots, 9$.

212. $14-4q$ и $2+3q$, $q=0, 1, 2, 3$.

213. По условию $15x+20y+30z=500$ и $x+y+z=18$, откуда $y+3z=46$, $y\equiv1 \pmod 3$ или $y=1+3t$. Значит, $3z=45-3t$ и $z=15-t$. Теперь имеем $x+16+2t=18$ или $x=2-2t$. Натуральное решение имеем лишь при $t=0$. Ответ: $x=2$, $y=1$, $z=15$.

214. 1) Из первого сравнения следует, что $x^{101}\equiv 2x \pmod{73}$. Используя транзитивность сравнений, имеем $2x\equiv 69 \pmod{73}$ или $x\equiv 71 \pmod{73}$. Проверка показывает, что найденные значения неизвестного удовлетворяют условию задачи. 2) $x\equiv 5 \pmod{29}$.

215. При $(a_0, m)=1$ сравнение $a_0x\equiv 1 \pmod{m}$ имеет единственное решение $x\equiv x_0 \pmod{m}$, где $(x_0, m)=1$. Данное сравнение равносильно сравнению $\sum_{i=0}^{n} x_0a_ix^{n-i}\equiv 0 \pmod{m}$. Заменяя коэффициент x_0a_0 единицей, получаем $x^n+\sum_{i=1}^{n} b_ix^{n-i}\equiv 0 \pmod{m}$, где $b_i=x_0a_i$ $(i=1, 2, \ldots, n)$.

216. Подстановка дает $a_0y^n+(na_0t+a_1)y^{n-1}+\ldots+(a_0t^n+a_1t^{n-1}+\ldots+a_n)\equiv 0 \pmod{m}$. Остается выбрать значение t так, чтобы $na_0t+a_1\equiv 0 \pmod{m}$. Но это всегда возможно при $(na_0, m)=1$.

217. При любом целом значении x имеем $x^{p-1}-1\equiv (x-1)\times(x-2)\ldots(x-p+1) \pmod{p}$. При $x=0$ получаем сравнение Вильсона.

Следует отметить, что верна и обратная теорема: если $(m-1)!+1\equiv 0 \pmod{m}$, то m — число простое (в противном случае простой делитель m должен быть делителем 1, что невозможно). В дальнейшем под теоремой Вильсона подразумевается утверждение: чтобы число m было простым, необходимо и достаточно, чтобы $(m-1)!+1\equiv 0 \pmod{m}$.

218. 1) Умножить части сравнения Вильсона на a и сложить почленно с $a^p\equiv a \pmod{p}$. 2) Перемножить почленно сравнения $(p-1)!\equiv -1 \pmod{p}$ и $a^p\equiv a \pmod{p}$.

219. $(p-1)!+1=(p-2)!(p-1)+1 = (p-2)!p-[(p-2)!-1]\equiv 0 \pmod{p}$, откуда $(p-2)!-1\equiv 0 \pmod{p}$.

220. Число p — простое тогда и только тогда, когда $4[(p-1)!+1]+p\equiv 0 \pmod{p}$ (следствие теоремы Вильсона). Остается доказать, что $p+2$ — число простое тогда и только тогда, когда $4[(p-1)!+1]+p\equiv 0 \pmod{p+2}$. С этой целью умножим части очевидного сравнения $p\equiv -2 \pmod{p+2}$ на $p+1$. Получаем $p(p+1)\equiv -2(p+1)=-2[(p+2)-1]\equiv 2 \pmod{p+2}$. Части полученного сравнения умножим на $2(p-1)!$:

$$2(p+1)!\equiv 4(p-1)! \pmod{p+2}.$$

К частям последнего сравнения прибавим по $p+4$:

$$2[(p+1)!+1]+(p+2)\equiv 4\ [(p-1)!+1]+p \pmod{p+2}.$$

По теореме Вильсона $p+2$ — число простое тогда и только тогда, когда $(p+1)!+1\equiv 0 \pmod{p+2}$ и, следовательно,

$$2[(p+1)!+1]+p+2\equiv 0 \pmod{p+2},$$

откуда $4[(p+1)!+1]+p\equiv 0 \pmod{p+2}$.

221. При $p=4k+1$ сравнение Вильсона (задача 217) имеет вид $(4k)!\equiv -1 \pmod{p}$. По данному модулю верны следующие $2k$ сравнений: $2k+1\equiv -2k$, $2k+2\equiv -(2k-1)$, ..., $4k-1\equiv -2$, $4k\equiv -1$, поэтому $(4k)!\equiv[(2k)!]^2\equiv -1 \pmod{p}$, откуда видно, что сравнение $x^2+1\equiv 0 \pmod{p=4k+1}$ имеет решения $x\equiv\pm(2k)! \pmod{p}$. Сравнение $x^2+1\equiv 0 \pmod{13=4\cdot 3+1}$ имеет решения $x\equiv\pm 6! \pmod{13}$. Так как $6!\equiv 5 \pmod{13}$, то полученные решения могут быть записаны в виде $x\equiv\pm 5 \pmod{13}$.

222. По условию $p-1 \vdots n$, поэтому имеем тождество $x^{p-1}-1=(x^n-1)Q(x)$, где $Q(x)$ — полином степени $p-1-n$ с целыми коэффициентами. Следовательно, сравнение $(x^n-1)Q(x)\equiv 0 \pmod{p}$ имеет $p-1$ решений (задача 191). Сравнения $x^n-1\equiv 0 \pmod{p}$ и $Q(x)\equiv 0 \pmod{p}$ имеют соответственно $\alpha\leqslant n$ и $\beta\leqslant p-1-n$ решений, причем $\alpha+\beta=p-1$. Если $\alpha<n$, то $\beta>p-1-n$, что невозможно. Значит, $\alpha=n$.

223. Общее число решений сравнений $\varphi(x)\equiv 0 \pmod{p}$ и $\psi(x)\equiv 0 \pmod{p}$ равно числу решений сравнений $f(x)\equiv 0 \pmod{p}$, причем сумма показателей степеней первых двух сравнений равна показателю степени третьего сравнения. Таким образом, если бы одно из сравнений $\varphi(x)\equiv 0 \pmod{p}$ или $\psi(x)\equiv 0 \pmod{p}$ имело решений меньше показателя его степени, то другое должно было бы иметь решений больше показателя его степени, что невозможно. Значит, число решений каждого из рассматриваемых сравнений равно показателю его степени.

224. Воспользоваться сравнением $x^{p-1}\equiv 1 \pmod{p}$ и применить теорему задачи 223.

225. Рассмотреть тождество $x^p-x=f(x)\cdot Q(x)+R(x)$, где $Q(x)$ и $R(x)$ — полиномы с целыми коэффициентами, причем степень $Q(x)$ равна $p-n$ и степень $R(x)$ не больше $n-1$.

Если данное сравнение имеет n решений, то все они являются решениями сравнения $R(x)\equiv 0 \pmod{p}$, что возможно только тогда, когда все коэффициенты $R(x)$ кратны p. Если известно, что все коэффициенты $R(x)$ кратны p, то имеем тождественное сравнение $f(x)\cdot Q(x)\equiv 0 \pmod{p}$, откуда данное сравнение имеет n решений (задача 223).

226. 2) Данное сравнение равносильно сравнению $x^3+x^2-3x+1\equiv 0 \pmod{7}$. Все коэффициенты остатка $-49x^2+70x-21$ от деления x^7-x на x^3+x^2-3x+1 кратны 7, поэтому данное сравнение имеет три решения. Это служит контрольным моментом при испытании системы остатков по модулю 7. Имеем: $x\equiv 1;\ 2;\ 3 \pmod{7}$.

227. 1) $x\equiv 3;\ 1;\ 8 \pmod{9}$. 2) Необходимо, чтобы $x^3+2x+3\equiv 0 \pmod{5}$, откуда $x\equiv 1;\ 2;\ 4 \pmod{5}$ или $x=1+5q;\ 2+5q;\ 4+5q$.

При $x=1+5q$ данное сравнение дает $5q+3\equiv 0 \pmod{25}$, откуда видно, что значений q, при которых $x=1+5q$ удовлетворяет данному сравнению, не существует.

При $x=4+5q$, находим $q=3+5t$, откуда $x=17+25t$. Подстановка $x=4+5q$, приводит к тождественному сравнению относительно q, следовательно, все эти значения x удовлетворяют исходному сравнению. Таким образом, исходное сравнение имеет решения:

$$x\equiv 17;\ 4;\ 9 \pmod{25}.$$

228. Если данное сравнение имеет решение, то $(x, 2)=1$ или $x=2q+1$; но тогда $4q^2+4q+1\equiv a \pmod{4}$, откуда $a\equiv 1 \pmod{4}$. Если известно, что $a\equiv 1 \pmod{4}$, то данное сравнение равносильно сравнению $x^2\equiv 1 \pmod{4}$, имеющему решения $x\equiv\pm 1 \pmod{4}$.

229. Если данное сравнение имеет решение, то $x=2q+1$ и $4q^2+4q+1=4q(q+1)+1\equiv a \pmod{8}$, откуда $a\equiv 1 \pmod{8}$.

Если известно, что $a\equiv 1 \pmod 8$, то данное сравнение равносильно сравнению $x^2\equiv 1 \pmod 8$, имеющему 4 решения: $x\equiv\pm 1$; $\pm 3 \pmod 8$.

230. Если данное сравнение имеет решение(то тем более имеет решение сравнение $x^2\equiv a \pmod 8$, откуда $a\equiv 1 \pmod 8$ (задача 229). Если известно, что $a\equiv 1 \pmod 8$, то при $\alpha=3$ данное сравнение имеет решение (задача 229). Допустим, что решение $x\equiv x_0 \pmod{2^\alpha}$ существует при некотором $\alpha\geqslant 3$. Тогда

$$x^2-a\,|_{x=x_0+2^{\alpha-1}\cdot y}=x_0^2-a+2^\alpha\cdot x_0\cdot y+2^{2(\alpha-1)}\cdot y^2=2^\alpha\,(q+x_0y)+$$

$$+2^{2(\alpha-1)}\cdot y^2\equiv 2^\alpha(q+x_0y) \pmod{2^{\alpha+1}},$$

так как при $\alpha\geqslant 3$ имеем $\alpha+1\leqslant 2(\alpha-1)$. Таким образом, чтобы $x^2\equiv a \pmod{2^{\alpha+1}}$, достаточно выбрать значение y так, чтобы $2^\alpha\,(q+x_0y)\equiv 0 \pmod{2^{\alpha+1}}$ или $x_0y\equiv -q \pmod 2$, что вполне возможно, так как $(x_0, 2)=1$. Итак, если $a\equiv 1 \pmod 8$, то сравнение $x^2\equiv a \pmod{2^\alpha}$ имеет решение при любом $\alpha\geqslant 3$. Теорема доказана полностью.

231. Пусть x и x_0 — различные нечетные числа, удовлетворяющие данному сравнению, причем x — произвольное такое число. Тогда $x^2-x_0^2\equiv(x-x_0)(x+x_0)\equiv 0 \pmod{2^\alpha}$, откуда $\frac{x-x_0}{2}\cdot\frac{x+x_0}{2}\equiv$ $\equiv 0 \pmod{2^{\alpha-2}}$. Так как разность чисел $\frac{x+x_0}{2}$ и $\frac{x-x_0}{2}$ нечетна, то сами они — числа различной четности. Поэтому для x имеем две возможности: либо $\frac{x-x_0}{2}\equiv 0 \pmod{2^{\alpha-2}}$, либо $\frac{x+x_0}{2}\equiv 0 \pmod{2^{\alpha-2}}$.

Отсюда имеем 4 решения: $x\equiv\pm x_0$; $\pm x_0+2^{\alpha-1} \pmod{2^\alpha}$. Например, сравнение $x^2\equiv 9 \pmod{16}$ имеет два очевидных решения: $x\equiv\pm 3 \pmod{16}$. По выведенным формулам легко найти остальные два решения: $x\equiv\pm 3+2^3\equiv\pm 5 \pmod{16}$.

З а м е ч а н и е. При $(a, 2)>1$ сравнение $x^2\equiv a \pmod{2^\alpha}$ может иметь меньше четырех решений. Так, сравнение $x^2\equiv 4 \pmod 8$ имеет только два решения: $x\equiv\pm 2 \pmod 8$.

232. При $a\equiv 2 \pmod 3$ из данного сравнения следует $x^2\equiv$ $\equiv 2 \pmod 3$. Но полученное сравнение не имеет решений, поэтому можно сделать вывод, что при $a\equiv 2 \pmod 3$ и данное сравнение не имеет решений. Значит, чтобы данное сравнение имело решение, необходимо, чтобы $a\equiv 1 \pmod 3$. Чтобы убедиться в достаточности этого условия, следует рассмотреть сравнение $x^2\equiv 1+3q \pmod 9$, откуда $x^2\equiv 1 \pmod 3$ и $x=\pm 1+3t$. Подстановка в сравнение $x^2\equiv 1+3q \pmod 9$ дает $t\equiv\mp q+3k$, откуда $x=\pm 1\mp 3q+9k$ или $x\equiv\pm 1\mp 3q \pmod 9$. Таким образом, при $a=1+3q$ данное сравнение имеет два решения.

Например, при $q=1$ (т. е. при $a=4$) данное сравнение принимает вид $x^2\equiv 4 \pmod 9$ и имеет решения: $x\equiv\pm 2 \pmod 9$.

233. $a\equiv 0$; 1; 4 $\pmod 5$. Для упражнения полезно записать ответ по данному модулю 25.

234. Дано сравнение вида $x^2 \equiv a \pmod{2^\alpha}$, где $\alpha=5$. $17 \equiv 1 \pmod 8$ и данное сравнение имеет 4 решения (задачи 230 и 231). Подбором легко найти, что в качестве x_0 можно взять 7. Таким образом, имеем: $x \equiv \pm 7$; $\pm 7+2^4 \equiv \pm 7$; $\pm 9 \pmod{32}$.

235. Так как $(x^2, p^2)=(-p, p^2)=p$, то $x=py$, откуда $p^2y^2 \equiv -p \pmod{p^2}$ или $0 \equiv -p \pmod{p^2}$, что невозможно.

236. 1) $x \equiv -3 \pmod{55}$; 2) решений нет; 3) $x \equiv 20 \pmod{42}$.

237. 1) $x \equiv 11 \pmod{30}$. 2) Первые два сравнения равносильны соответственно сравнениям $x \equiv -1 \pmod 3$ и $x \equiv -1 \pmod 2$ и могут быть отброшены как следствия третьего сравнения системы. Таким образом, третье сравнение системы является ее решением. 3) Из третьего сравнения системы следует, что $x=1+3q$. Подстановка в первое сравнение дает $q=1+7q_1$, откуда $x=4+21q_1$. Подстановка во второе сравнение системы дает $q_1=5q_2$, откуда $x=4+105q_2$ или $x \equiv 4 \pmod{105}$. 4) Данная система приводится к виду

$$\begin{cases} x \equiv 40 \pmod{251}, \\ x \equiv 382 \pmod{401}, \\ x \equiv 252 \pmod{907}, \end{cases}$$

откуда $x \equiv 7777777 \pmod{91290457}$.

238. Задача приводит к системе

$$\begin{cases} x \equiv 1 \pmod{12}, \\ x \equiv 0 \pmod{5}, \end{cases}$$

откуда $x \equiv 25 \pmod{60}$.

239. 86.

240. Задача приводит к системе

$$\begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{5}, \\ x \equiv 5 \pmod{6}, \\ x \equiv 0 \pmod{7}, \end{cases}$$

откуда $x \equiv 119 \pmod{420}$.

Замечание. Сравнение $x \equiv 1 \pmod 2$ или $x \equiv 3 \pmod 2$ может быть сразу же отброшено как следствие сравнения $x \equiv 3 \pmod 4$. Аналогичное соображение позволяет отбросить сравнение $x \equiv 2 \pmod 3$.

241. 299 и 439.

242. Следует решить систему сравнений $4x \equiv 9 \pmod 7$, $2x \equiv 15 \pmod 9$ и $5x \equiv 12 \pmod{13}$, откуда $x \equiv 291 \pmod{819}$. Ординаты точек находятся с помощью данных уравнений прямых.

243. 1) $x \equiv 4a-3 \pmod{24}$, $a \equiv 1 \pmod 2$. 2) $x \equiv 8-3a \pmod{24}$, $a \equiv 0 \pmod 2$. 3) Система имеет решение тогда и только тогда, когда $a \equiv 8 \pmod 7$, где $7=(21, 35)$, или когда $a=1+7q$.

Подстановка $x=1+7q+35t$ (см. третье сравнение системы) во второе сравнение приводит к $t=q-1+3t_1$ и $x=42q-34+105t_1$. Подстановка в первое сравнение дает $t_1=2q-1+6t_2$, откуда $x \equiv 252q-139 \pmod{630}$ или $x \equiv 36a-175 \pmod{630}$, где $a \equiv 1 \pmod 7$.

Второй способ решения. Подстановка $x=a+35t$ во второе сравнение приводит к $35t \equiv 8-a \pmod{21}$, $5t \equiv \frac{8-a}{7} \pmod 3$

или $t=\frac{a-8}{7}+3t_1$ и $x=6a-40+105t_1$; подстановка в первое сравнение дает $t_1=2a-3+6t_2$, откуда $x\equiv 216a-355 \pmod{630}$, где $a\equiv 1 \pmod 7$.

Замечание. Нетрудно проверить, что при $a\equiv 1 \pmod 7$ имеем $216a-355\equiv 36a-175 \pmod{630}$.

4) $x\equiv 15a+21b-35c \pmod{105}$; 5) $x\equiv 2 \pmod{12m}$.

244. 1) Необходимо и достаточно, чтобы

$$\begin{cases} a\equiv 1 \pmod 2, \\ a\equiv 2 \pmod 3, \end{cases}$$

откуда $a\equiv 5 \pmod 6$.

2) Первое сравнение системы имеет решение тогда и только тогда, когда $a\equiv 0 \pmod 2$ или $a=2q$. При этих значениях a данная система равносильна следующей:

$$\begin{cases} x\equiv q \pmod 2, \\ x\equiv 8 \pmod{10}; \end{cases}$$

последняя имеет решение лишь при $q\equiv 0 \pmod 2$ или $q=2q_1$, откуда $a=4q_1$ или $a\equiv 0 \pmod 4$.

245. Необходимо и достаточно, чтобы $7-3=4\not\equiv 0 \pmod{(6,m)}$. Если, например, $(6, m)=3$, то можно взять $m=15$.

246. $(m_1, m_2)=(m_1, 4)=(m_2, 4)=1$.

247. 1) $x\equiv 24 \pmod{28}$; 2) $x\equiv 54 \pmod{95}$; 3) $x\equiv 39 \pmod{77}$; 4) $x\equiv -9 \pmod{45}$.

248. Числа x_1 и x_2 существуют, так как при $(m_1, m_2)=1$ сравнения $m_2x\equiv 1 \pmod{m_1}$ и $m_1x\equiv 1 \pmod{m_2}$ имеют решения. Доказательство сводится к обычной проверке: подставляя $x=m_2a_1x_1+$ $+m_1a_2x_2$, например, в первое сравнение, получаем $m_2a_1x_1\equiv$ $\equiv a_1 \pmod{m_1}$, что верно, так как является следствием данного сравнения $m_2x_1\equiv 1 \pmod{m_1}$.

Замечание. Данная теорема допускает обобщение: система сравнений $x\equiv a_i \pmod{m_i}$, где $i=1, 2, \ldots, k$ и $(m_{i_1}, m_{i_2})=1$, имеет единственное решение $x\equiv \sum_{i=1}^{k}\mu_i a_i x_i \pmod{\prod_{i=1}^{k} m_i}$, где $\mu_1=$ $=\frac{\Pi m_i}{m_1}$, $\mu_2=\frac{\Pi m_i}{m_2}, \ldots, \mu_k=\frac{\Pi m_i}{m_k}$ и x_i — значение неизвестного, удовлетворяющее соответственно сравнению $\mu_i x\equiv 1 \pmod{m_i}$.

249. 1) $x\equiv -3 \pmod{30}$; 2) $x\equiv 201 \pmod{990}$.

250. 1) Данное сравнение равносильно системе

$$\begin{cases} x^3+2x+3\equiv 0 \pmod 5, \\ x^3+2x+3\equiv 0 \pmod 3. \end{cases}$$

Второе сравнение этой системы равносильно сравнению $(x-1)x\cdot(x+1)\equiv 0 \pmod 3$ и, следовательно, является тождественным. Задача сводится к решению сравнения $x^3+2x+3\equiv 0 \pmod 5$, откуда $x\equiv 2; 4 \pmod 5$. По данному модулю имеем $x\equiv 2; 7; 12; 4; 9; 14 \pmod{15}$.

2) Система сравнений $x^2 \equiv -1 \pmod 5$ и $x^2 \equiv -1 \pmod 4$ не имеет решений, так как не имеет решений второе ее сравнение. Данное сравнение не имеет решений.

3) Первое сравнение системы

$$\begin{cases} x^2 \equiv -1 \pmod 5, \\ x^2 \equiv -1 \pmod{17} \end{cases}$$

имеет решения $x \equiv \pm 2 \pmod 5$, второе — $x \equiv \pm 4 \pmod{17}$, поэтому задача сводится к решению следующих систем:

$$\begin{cases} x \equiv 2 \pmod 5, \\ x \equiv 4 \pmod{17}, \end{cases} \quad \begin{cases} x \equiv 2 \pmod 5, \\ x \equiv -4 \pmod{17}, \end{cases} \quad \begin{cases} x \equiv -2 \pmod 5, \\ x \equiv 4 \pmod{17}, \end{cases}$$

$$\begin{cases} x \equiv -2 \pmod 5, \\ x \equiv -4 \pmod{17}, \end{cases}$$

откуда $x \equiv \pm 13;\ \pm 47 \pmod{85}$.

251. 1) Первое сравнение системы является тождественным, поэтому задача сводится к решению сравнения $x^3 \equiv 2 \pmod 5$, откуда $x \equiv 3 \pmod 5$. 2) Оба сравнения системы являются тождественными, поэтому $x \equiv 0;\ 1;\ 2;\ 3;\ 4;\ 5 \pmod 6$, т. е. любое целое значение неизвестного удовлетворяет данной системе сравнений.

252. Задача приводит к системе

$$\begin{cases} x \equiv 3 \pmod 7, \\ x^2 \equiv 44 \pmod{7^2}, \\ x^3 \equiv 111 \pmod{7^3}. \end{cases}$$

Подстановка $x = 3 + 7q$ (см. первое сравнение) во второе сравнение дает $q = 2 + 7q_1$, откуда первым двум сравнениям системы удовлетворяют $x = 17 + 7^2 \cdot q_1$. Подстановка этих значений неизвестного в третье сравнение системы приводит к $q_1 = 7q_2$, откуда $x = 17 + 7^3 \cdot q_2$ ($q_2 = 0, 1, 2, \ldots$).

253. Задача приводит к системе

$$\begin{cases} x \equiv 1 \pmod m, \\ x^2 \equiv m + 1 \pmod{m^2}. \end{cases}$$

Подстановка $x = 1 + mq$ (см. первое сравнение) во второе сравнение приводит к $2q \equiv 1 \pmod m$, откуда $q = 2^{\varphi(m)-1} + mq_1$ и $x = 1 + m \cdot 2^{\varphi(m)-1} + m^2 \cdot q$, или $x \equiv 1 + m \cdot 2^{\varphi(m)-1} \pmod{m^2}$.

Замечание. Сравнение $2q \equiv 1 \pmod m$ может быть решено и так: $q \equiv \dfrac{m+1}{2} \pmod m$, откуда решение исходной системы имеет вид

$$x \equiv 1 + \frac{m(m+1)}{2} \pmod{m^2}.$$

Возникает задача: доказать, что $\dfrac{m(m+1)}{2} \equiv m \cdot 2^{\varphi(m)-1} \pmod{m^2}$.

Рекомендуется решить ее самостоятельно.

254. Задача приводит к системе

$$\begin{cases} x \equiv m - 1 \pmod m, \\ x^2 \equiv 1 \pmod{m^2}, \end{cases}$$

где $m \neq 1$ и $(m, 2) = 1$, откуда $x \equiv m - 1 + m \cdot (m-1)^{\varphi(m)-1} \pmod m$.

255. 1) Имеем $2x^3-5x^2+4x+11\equiv 0 \pmod{15}$ или

$$\begin{cases} 2x^3-5x^2+4x+11\equiv 0 \pmod 5, \\ 2x^3-5x^2+4x+11\equiv 0 \pmod 3). \end{cases}$$

Первое сравнение системы имеет решения $x\equiv 2;\ 4 \pmod 5$, а второе $x\equiv 1;\ 2 \pmod 3$.

Решая системы

$$\begin{cases} x\equiv 2 \pmod 5, \\ x\equiv 1 \pmod 3; \end{cases} \quad \begin{cases} x\equiv 2 \pmod 5, \\ x\equiv 2 \pmod 3; \end{cases} \quad \begin{cases} x\equiv 4 \pmod 5, \\ x\equiv 1 \pmod 3; \end{cases} \quad \begin{cases} x\equiv 4 \pmod 5, \\ x\equiv 2 \pmod 3; \end{cases}$$

находим $x\equiv 7;\ 2;\ 4;\ 14 \pmod{15}$.

Указанным в условии границам удовлетворяют $x=7;\ 2;\ 4;\ -1$. Соответствующие значения y находятся по данному уравнению.

2) $(-6, -61), (-1, -1), (1, 1), (6, 41)$.

256. 1) $\begin{cases} x\equiv 0, \\ y\equiv 2, \end{cases} \quad \begin{cases} x\equiv 1, \\ y\equiv 0, \end{cases} \quad \begin{cases} x\equiv 2 \\ y\equiv 1 \end{cases} \pmod 3$.

4) Первый способ. x — число четное. При $x\equiv 1 \pmod 6$ имеем $y\equiv 1 \pmod 3$, откуда получаем следующие два решения данного сравнения:

$$\begin{cases} x\equiv 1, \\ y\equiv 1; \end{cases} \quad \begin{cases} x\equiv 1 \\ y\equiv 4 \end{cases} \pmod 6.$$

Аналогично находятся остальные решения:

$$\begin{cases} x\equiv 3, \\ y\equiv 4; \end{cases} \quad \begin{cases} x\equiv 5, \\ y\equiv 1; \end{cases} \quad \begin{cases} x\equiv 5 \\ y\equiv 4 \end{cases} \pmod 6.$$

Второй способ. Необходимо, чтобы $2y\equiv 5 \pmod 3$, откуда $y\equiv 1 \pmod 3$ или $y\equiv 1;\ 4 \pmod 6$. Каждому из этих классов значений y соответствует три класса значений x, в чем легко убедиться подстановкой.

257. Имеем $ax\equiv c-by \pmod m$. При $(a, m)=1$ каждому из m классов значений y соответствует класс значений x и, следовательно, m решений данного сравнения.

258. Значения x должны удовлетворять условию $ax\equiv c(\mathrm{mod}\ \ d=(b, m))$, где $(a, d)=1$, откуда $x\equiv c{,}a^{\varphi(d)-1} \pmod d$ или $x\equiv x_0;\ x_0+d;\ x_0+2d;\ \ldots;\ x_0+\left(\frac{m}{d}-1\right)d \pmod m$, где x_0—одно из значений x из класса $x\equiv c\cdot a^{\varphi(d)-1} \pmod d$. Каждому из этих $\frac{m}{d}$ классов значений x соответствует сравнение вида $by\equiv B \pmod m$, где $B\equiv 0 \pmod d$, определяющее d классов значений y и, следовательно, d решений данного сравнения. Таким образом, данное сравнение имеет $d\cdot\frac{m}{d}=m$ решений.

259. 1) Имеем $2x\equiv 6y+5 \pmod{15}$ или $x\equiv 3y+10 \pmod{15}$, откуда

$$\begin{cases} x\equiv 10, \\ y\equiv 0; \end{cases} \quad \begin{cases} x\equiv 13, \\ y\equiv 1; \end{cases} \quad \ldots, \quad \begin{cases} x\equiv 7 \\ y\equiv 14 \end{cases} \pmod{15}.$$

2) $$\begin{cases} x\equiv -2, \\ y\equiv 0; \end{cases} \begin{cases} x\equiv 0, \\ y\equiv 1; \end{cases} \begin{cases} x\equiv 2, \\ y\equiv 2; \end{cases} \begin{cases} x\equiv 0 \\ y\equiv 3 \end{cases} \pmod 4.$$

260. При $c \equiv 0 \pmod d$ имеем: $\frac{a}{d}x+\frac{b}{d}y \equiv \frac{c}{d}\left(\mathrm{mod}\,\frac{m}{d}\right)$, где $\left(\frac{a}{d}, \frac{b}{d}, \frac{m}{d}\right)=1$. Следовательно, при $c \equiv 0 \pmod d$ данное сравнение имеет $\frac{m}{d}$ решений по модулю $\frac{m}{d}$ (задача 258). Каждое из этих решений по данному модулю разбивается на d^2 решений. Таким образом, по данному модулю исходное сравнение может иметь $d^2 \cdot \frac{m}{d} = md$ решений.

261. 1) Свободный член делится на $d=(3, 3, 6)=3$, следовательно, сравнение имеет $6 \cdot 3=18$ решений. Имеем $x+y \equiv 1 \pmod 2$, откуда

$$\begin{cases} x \equiv 0, \\ y \equiv 1; \end{cases} \begin{cases} x \equiv 1 \\ y \equiv 0 \end{cases} \pmod 2,$$

или по данному модулю:

$$\begin{cases} x \equiv 0, \\ y \equiv 1; \end{cases} \begin{cases} x \equiv 0, \\ y \equiv 3; \end{cases} \begin{cases} x \equiv 0, \\ y \equiv 5; \end{cases} \begin{cases} x \equiv 2, \\ y \equiv 1; \end{cases} \begin{cases} x \equiv 2, \\ y \equiv 3; \end{cases} \begin{cases} x \equiv 2 \\ y \equiv 5 \end{cases} \text{ и т. д.}$$

3) Имеем $2x+3y \equiv 5 \pmod 6$, откуда $2x \equiv 5 \pmod 3$, $x \equiv 1 \pmod 3$ или $x \equiv 1; 4 \pmod 6$. Каждый из этих классов значений x при помощи сравнения $2x+3y \equiv 5 \pmod 6$ определяет три класса значений y. Таким образом, получаем 6 решений:

$$\begin{cases} x \equiv 1, \\ y \equiv 1; \end{cases} \begin{cases} x \equiv 1, \\ y \equiv 3; \end{cases} \begin{cases} x \equiv 1, \\ y \equiv 5; \end{cases} \begin{cases} x \equiv 4, \\ y \equiv 1; \end{cases} \begin{cases} x \equiv 4, \\ y \equiv 3; \end{cases} \begin{cases} x \equiv 4 \\ y \equiv 5 \end{cases} \pmod 6.$$

Остается разбить эти решения на 24 решения по данному модулю 12.

262. 1) Имеем:

$$\begin{cases} x+3y \equiv 5 \\ x \equiv 3 \end{cases} \pmod 7,$$

откуда $x \equiv y \equiv 3 \pmod 7$.

2) Имеем $\begin{cases} 7x \equiv 1+8y, \\ y \equiv 3; \end{cases} \begin{cases} 7x \equiv 1+8y, \\ y \equiv 7; \end{cases} \begin{cases} 7x \equiv 1+8y \\ y \equiv 11 \end{cases} \pmod{12}$

или $\begin{cases} x \equiv 10, \\ y \equiv 3; \end{cases} \begin{cases} x \equiv 10, \\ y \equiv 7; \end{cases} \begin{cases} x \equiv 10 \\ y \equiv 11 \end{cases} \pmod{12}$.

3)—4) Решений нет.

5) $\begin{cases} x \equiv 0, \\ y \equiv 7; \end{cases} \begin{cases} x \equiv 4, \\ y \equiv 7; \end{cases} \begin{cases} x \equiv 8 \\ y \equiv 7 \end{cases} \pmod{12}$.

263. Если $b \equiv 0 \pmod{(a, m)=d}$, то первое сравнение определяет d классов значений x. Каждому из этих классов соответствует сравнение вида $b_1y \equiv B \pmod m$, которое может иметь $(b_1, m)=d_1$ решений, что дает d_1 решений системы. Таким образом, система может иметь максимум dd_1 решений.

264. 1) Первый способ. Умножая части второго сравнения на 2 и затем почленно вычитая, получаем $7x\equiv 1 \pmod 5$, откуда $x\equiv 3 \pmod 5$. Умножение частей первого сравнения на 4 и почленное вычитание дает $y\equiv 0 \pmod 5$. Проверка показывает, что

$$\begin{cases} x\equiv 3 \\ y\equiv 0 \end{cases} \pmod 5$$

является решением системы.

Второй способ. Из первого сравнения $x\equiv 3-2y \pmod 5$. Подстановка во второе сравнение дает $y\equiv 0 \pmod 5$. Этим значениям y соответствуют $x\equiv 3 \pmod 5$. Проверка показывает, что найденные значения неизвестных составляют решение данной системы. 2) $\begin{cases} x\equiv 1 \\ y\equiv 2 \end{cases} \pmod 5$. 3) $\begin{cases} x\equiv 100 \\ y\equiv 101 \end{cases} \pmod{143}$. 4) Множество решений системы совпадает с множеством решений одного из данных сравнений:

$$\begin{cases} x\equiv 4, \\ y\equiv 0; \end{cases} \begin{cases} x\equiv 2, \\ y\equiv 1; \end{cases} \begin{cases} x\equiv 0, \\ y\equiv 2; \end{cases} \begin{cases} x\equiv 3, \\ y\equiv 3; \end{cases} \begin{cases} x\equiv 1 \\ y\equiv 4 \end{cases} \pmod 5.$$

265. 1) $\begin{cases} x\equiv 5, \\ y\equiv 0; \end{cases} \begin{cases} x\equiv 2 \\ y\equiv 3 \end{cases} \pmod 6$. 2) Система не имеет решений, так как не имеет решений второе ее сравнение. 3) Множество решений системы совпадает с множеством решений сравнения $x-y\equiv 2 \pmod 6$. 4) $\begin{cases} x\equiv 1, \\ y\equiv 2; \end{cases} \begin{cases} x\equiv 4 \\ y\equiv 2 \end{cases} \pmod 6$.

266. Из (1) следует $\begin{cases} Dx\equiv D_1 \\ Dy\equiv D_2 \end{cases} \pmod m$, где $D_1=\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}$, $D_2=\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}$. При $(D, m)=1$ имеем: $\begin{cases} x\equiv D_1\cdot D^{\varphi(m)-1} \\ y\equiv D_2\cdot D^{\varphi(m)-1} \end{cases} \pmod m$.

Подстановка этих значений неизвестных в (1) показывает, что они составляют единственное решение (1).

267. По крайней мере один из определителей D_1 и D_2 не делится на d.

Система $\begin{cases} 3x-2y\equiv 5 \\ 5x+2y\equiv 1 \end{cases} \pmod{20}$

приводит к $\begin{cases} 16x\equiv 12 \\ 16y\equiv -22 \end{cases} \pmod{20}$,

где $-22\not\equiv 0 \pmod{(16, 20)=4}$. Следовательно, класса значений y, составляющего решение данной системы, не существует. Данная система не имеет решений.

268. 1) $\begin{cases} x\equiv -1 \\ y\equiv 3 \end{cases} \pmod 6$. 2) Не имеет решений.

269. При данном условии второе сравнение системы (1) является следствием первого ее сравнения: $a_1a_2x+a_2b_1y\equiv \equiv a_2c_1 \pmod m$, откуда при

$$\left.\begin{matrix} a_2b_1\equiv a_1b_2 \\ a_2c_1\equiv a_1c_2 \end{matrix}\right\} \pmod m$$

имеем $a_1a_2x+a_1b_2y\equiv a_1c_2 \pmod m$ и, наконец, $a_2x+b_2y\equiv c_2 \pmod m$ в силу $(a_1, m)=1$.

Замечание. В условии данной задачи речь идет о коэффициенте именно при x лишь для определенности. Смысл предлагаемой теоремы таков: если при условии $D\equiv D_1\equiv D_2\equiv 0 \pmod m$ какой-нибудь из коэффициентов при неизвестном в одном из сравнений взаимно прост с модулем, то система (1) равносильна этому сравнению.

270. 1) Для данной системы выполняется условие $D\equiv D_1\equiv D_2\equiv 0 \pmod 8$ и в первом сравнении коэффициент при x взаимно прост с модулем (как, впрочем, и коэффициент при y). Следовательно, решение данной системы сводится к решению ее первого сравнения (задача 269). Имеем по данному модулю:

$$\begin{cases}x\equiv 0,\\ y\equiv 2;\end{cases} \begin{cases}x\equiv 1,\\ y\equiv 3;\end{cases} \begin{cases}x\equiv 2,\\ y\equiv 4;\end{cases} \begin{cases}x\equiv 3,\\ y\equiv 5;\end{cases} \begin{cases}x\equiv 4,\\ y\equiv 6;\end{cases} \begin{cases}x\equiv 5,\\ y\equiv 7;\end{cases} \begin{cases}x\equiv 6,\\ y\equiv 0;\end{cases} \begin{cases}x\equiv 7,\\ y\equiv 1.\end{cases}$$

Замечание. Легко убедиться в том, что второе сравнение данной системы действительно является следствием первого: оно равносильно сравнению $3x+y\equiv 2 \pmod 4$ или $y\equiv x+2 \pmod 4$, откуда $y\equiv x+2;\ x+6 \pmod 8$; первая из этих возможностей и равносильна первому сравнению данной системы.

2) В этой системе при условии $D\equiv D_1\equiv D_2\equiv 0 \pmod 3$ оба коэффициента при x взаимно просты с модулем. Следовательно, эта система равносильна любому из своих сравнений. Ответ:

$$\begin{cases}x\equiv 0,\\ y\equiv 1;\end{cases} \begin{cases}x\equiv 1,\\ y\equiv 2;\end{cases} \begin{cases}x\equiv 2\\ y\equiv 0\end{cases} \pmod 3.$$

271. 1) Из первого сравнения следует $x+3y\equiv -1 \pmod 4$ или $y\equiv x+1+4i \pmod{12}$, где $i=0, 1, 2$. Подстановка во второе сравнение приводит к $x\equiv i-1;\ i+2;\ i+5;\ i+8 \pmod{12}$. Таким образом, система имеет 12 решений. Например, при $i=0$ получаем следующие 4 решения:

$$\begin{cases}x\equiv -1,\\ y\equiv 0;\end{cases} \begin{cases}x\equiv 2,\\ y\equiv 3;\end{cases} \begin{matrix}x\equiv 5,\\ y\equiv 6;\end{matrix} \begin{cases}x\equiv 8\\ y\equiv 9\end{cases} \pmod{12}.$$

2) Из первого сравнения следует $y\equiv x-1+3i \pmod 6$, где $i=0; 1$. Подстановка во второе сравнение приводит к $i\equiv 0 \pmod 2$, откуда $i=0$. Итак, данная система равносильна сравнению $y\equiv x-1 \pmod 6$, откуда

$$\begin{cases}x\equiv 0,\\ y\equiv -1;\end{cases} \begin{cases}x\equiv 1,\\ y\equiv 0;\end{cases} \begin{cases}x\equiv 2,\\ y\equiv 1;\end{cases} \begin{cases}x\equiv 3,\\ y\equiv 2;\end{cases} \begin{cases}x\equiv 4,\\ y\equiv 3;\end{cases} \begin{cases}x\equiv 5\\ y\equiv 4\end{cases} \pmod 6.$$

3) Почленное сложение данных сравнений дает $x\equiv 2;\ 7 \pmod{10}$. Подстановка этих классов значений x в данную систему показывает, что лишь второму из них соответствует два класса значений y, а именно $y\equiv 3;\ 8 \pmod{10}$. Данная система имеет два решения:

$$\begin{cases}x\equiv 7,\\ y\equiv 3;\end{cases} \begin{cases}x\equiv 7\\ y\equiv 8\end{cases} \pmod{10}.$$

4) $$\begin{cases}x\equiv 13,\\ y\equiv 3;\end{cases} \begin{cases}x\equiv 13\\ y\equiv 10\end{cases} \pmod{14}.$$

272. 1) Из первого сравнения следует $y\equiv 1-x+4i \pmod{12}$, где $i=0;\ 1;\ 2$. Подстановка во второе сравнение дает $3x\equiv 6-8i \pmod{12}$, откуда $i=0$.

Итак, $\begin{cases} 3x\equiv 6 \\ y\equiv 1-x \end{cases} \pmod{12}$,

или $\begin{cases} x\equiv 2, \\ y\equiv -1; \end{cases}$ $\begin{cases} x\equiv 6, \\ y\equiv -5; \end{cases}$ $\begin{cases} x\equiv 10 \\ y\equiv -9 \end{cases} \pmod{12}$.

2) Из первого сравнения следует $y\equiv 2x+1+4i \pmod{12}$, где $i=0;\ 1;\ 2$. Подстановка во второе сравнение дает $x\equiv 2i;\ 2i+3;\ 2i+6;\ 2i+9 \pmod{12}$. Итак, данная система имеет 12 решений. Например, при $i=0$ имеем следующие 4 решения:

$$\begin{cases} x\equiv 0, \\ y\equiv 1; \end{cases} \begin{cases} x\equiv 3, \\ y\equiv 7; \end{cases} \begin{cases} x\equiv 6, \\ y\equiv 1; \end{cases} \begin{cases} x\equiv 9 \\ y\equiv 7 \end{cases} \pmod{12}.$$

3) $\begin{cases} x\equiv 0, \\ y\equiv 1; \end{cases} \begin{cases} x\equiv 2, \\ y\equiv -1; \end{cases} \begin{cases} x\equiv 4, \\ y\equiv -3; \end{cases} \begin{cases} x\equiv 6, \\ y\equiv -5; \end{cases} \begin{cases} x\equiv 8, \\ y\equiv -7; \end{cases} \begin{cases} x\equiv 10 \\ y\equiv -9 \end{cases} \pmod{12}$.

4) Данная система равносильна сравнению $y\equiv x-1 \pmod 6$.

5) $\begin{cases} x\equiv -1, \\ y\equiv 0; \end{cases} \begin{cases} x\equiv 2 \\ y\equiv 3 \end{cases} \pmod 6$.

273. $[33,\ 21]=231$. Из первого сравнения следует $y\equiv 3-5x+33i \pmod{231}$, где $i=0;\ 1;\ \ldots,\ 6$. Подстановка во второе сравнение дает $9x\equiv 5+66i \pmod{21}$. Последнее сравнение не имеет решений, так как $5+66i\not\equiv 0 \pmod 3$.

274. Пусть $[m_1,\ m_2]=m$ и $m=m_1q_1=m_2q_2$. Данная система равносильна системе

$$\begin{cases} a_1q_1x+b_1q_1y\equiv c_1q_1 \\ a_2q_2x+b_2q_2y\equiv c_2q_2 \end{cases} \pmod m,$$

из которой следует $\begin{cases} q_1q_2Dx\equiv q_1q_2D_1 \\ q_1q_2Dy\equiv q_1q_2D_2 \end{cases} \pmod m$,

или $\begin{cases} Dx\equiv D_1 \\ Dy\equiv D_2 \end{cases} \pmod d$,

где $D=\begin{vmatrix} a_1 b_1 \\ a_2 b_2 \end{vmatrix}$, $D_1=\begin{vmatrix} c_1 b_1 \\ c_2 b_2 \end{vmatrix}$, $D_2=\begin{vmatrix} a_1 c_1 \\ a_2 c_2 \end{vmatrix}$ и $d=\dfrac{m}{q_1q_2}=(m_1m_2)$.

Пусть $(D,\ d)=\delta$. Тогда искомым критерием будет $D_1\equiv D_2\equiv 0 \pmod\delta$.

275. Условие задачи можно выразить системой

$$\begin{cases} \overline{xy2}\equiv 0 \pmod 4, \\ \overline{xy2}\equiv 0 \pmod 7, \end{cases} \text{ или } \begin{cases} y+1\equiv 0 \pmod 2, \\ 2x+3y+2\equiv 0 \pmod 7). \end{cases}$$

Из первого сравнения следует $y=1+2n$, где $n=0;\ 1;\ 2;\ 3;\ 4$. Подстановка во второе сравнение дает $x\equiv 1+4n \pmod 7$.

Ответ: 112, 812, 532, 252, 952, 672, 392.

276. Условие задачи можно выразить системой

$$\begin{cases} \overline{xy9z} \equiv 0 \pmod 3, \\ \overline{xy9z} \equiv 0 \pmod 4, \\ \overline{xy9z} \equiv 0 \pmod{11}, \end{cases} \text{ или } \begin{cases} x+y+z \equiv 0 \pmod 3, \\ 1+z \equiv 0 \pmod 4, \\ -x+y+2+z \equiv 0 \pmod{11}. \end{cases}$$

Из первого сравнения следует, что $z_1=3$ и $z_2=7$. При $z_1=3$ имеем систему:

$$\begin{cases} x+y \equiv 0 \pmod 3, \\ -x+y=6 \pmod{11}, \end{cases}$$

откуда $x=3$, $y=9$ и искомое число есть 3993. При $z_2=7$ имеем систему:

$$\begin{cases} x+y+1 \equiv 0 \pmod 3, \\ -x+y+9 \equiv 0 \pmod{11}, \end{cases}$$

откуда $x=3$, $y=5$ и $x=6$, $y=7$. Таким образом, имеем еще два числа, отвечающие условиям задачи: 3597 и 6797.

277. Задача приводит к системе

$$\begin{cases} 1000+100x+10y+2 \equiv 0 \\ 1000x+120+y \equiv 0 \end{cases} \pmod 7,$$

откуда $x=6$ и $y=5$. Имеем единственное решение: 1652 и 6125.

278. Соответствующая система

$$\begin{cases} 100x+10y+2 \equiv 0 \\ 200+10x+y \equiv 0 \end{cases} \pmod 7$$

решений не имеет.

279. 1) $x=k+5n$, $y=2k-2+10n$, $z=1-k-5n$, где $k=0; 1; 2; 3; 4$ и n—произвольное целое число.

2) Имеем систему сравнений

$$\begin{cases} x-y \equiv 1 \pmod 3, \\ x+y \equiv 1 \pmod 2. \end{cases}$$

Из первого сравнения $y \equiv x-1+3i \pmod 6$, где $i=0; 1$. Подстановка во второе сравнение системы дает $2x \equiv 2-3i \pmod 2$, откуда $3i \equiv 0 \pmod 2$ и $i=0$. Следовательно,

$$\begin{cases} x \equiv k \pmod 6, \\ y \equiv k-1 \pmod 6), \quad k=0; 1; 2; 3; 4; 5. \end{cases}$$

или $x=k+6n$, $y=k-1+6m$, где n и m—целые числа. Подставляя в уравнения, имеем $z=2n-2m=k-1+3n+3m$, откуда $n=1-k-5m$. Таким образом, решения данной системы уравнений имеют вид

$$x=6-5k-30m, \quad y=k-1+6m, \quad z=2-2k-12m,$$

где $k=0; 1; 2; 3; 4; 5$ и m—произвольное целое число.

280. Задачу можно решить при помощи системы сравнений:

$$\begin{cases} 3x-y+1 \equiv 0 \pmod 7, \\ 2x+3y-1 \equiv 0 \pmod 7), \end{cases}$$

откуда $\begin{cases} x \equiv 3 \\ y \equiv 5 \end{cases} \pmod 7.$

281. 1) $(2x+2)^2 \equiv 1 \pmod 5$, откуда $x \equiv 2;\ 1 \pmod 5$;
2) $(3x+1)^2 \equiv 4 \pmod 7$, откуда $x \equiv 5;\ 6 \pmod 7$;
3) $(2x-1)^2 \equiv 3 \pmod 7$, не имеет решений;
4) $(6x-1)^2 \equiv 1 \pmod 5$, откуда $x \equiv 2;\ 0 \pmod 5$.

Замечание. Приведение данных сравнений к двучленному может быть осуществлено при помощи подстановки $x=y+t$. Например, в случае сравнения 1) эта подстановка дает $2y^2-(t+1)y+2t^2-t-1\equiv 0 \pmod 5$; при $t+1\equiv 0 \pmod 5$ или $t\equiv 4 \pmod 5$ имеем: $2y^2+2\equiv y^2+1\equiv 0 \pmod 5$, откуда $y\equiv \pm 2 \pmod 5$ и $x=y+t\equiv 2;\ 1 \pmod 5$.

282. Данное сравнение равносильно сравнению $(2ax+b)^2 \equiv \equiv b^2-4ac \pmod p$, которое разрешимо относительно $2ax+b$ тогда и только тогда, когда $(b^2-4ac)^{\frac{p-1}{2}} \equiv 1 \pmod p$ по критерию Эйлера.

283. Имеем: $(2ax+b)^2\equiv b^2-4ac \pmod p$, откуда $2ax+b\equiv \equiv 0 \pmod p$, или $x\equiv -b\cdot(2a)^{p-2} \pmod p$.

284. 1) Вопрос приводит к сравнению $x^2+2x+7\equiv 0 \pmod{55}$, или $(x+1)^2\equiv -6 \pmod{55}$, равносильному системе

$$\begin{cases} (x+1)^2\equiv 16 \pmod{11}, \\ (x+1)^2\equiv 4 \pmod 5. \end{cases}$$

Первое сравнение системы имеет решения: $x\equiv 3;\ 6 \pmod{11}$, а второе — $x\equiv 1;\ 2 \pmod 5$. Решение систем:

$$\begin{cases} x\equiv 3 \pmod{11}, \\ x\equiv 1 \pmod 5; \end{cases} \quad \begin{cases} x\equiv 3 \pmod{11}, \\ x\equiv 2 \pmod 5; \end{cases} \quad \begin{cases} x\equiv 6 \pmod{11}, \\ x\equiv 1 \pmod 5; \end{cases} \quad \begin{cases} x\equiv 6 \pmod{11}, \\ x\equiv 2 \pmod 5 \end{cases}$$

дает $x=36+55q;\ 47+55q;\ 6+55q;\ 17+55q$, где $q=0;\ 1;\ 2,\ \dots$.

2) Чтобы натуральное значение x удовлетворяло сравнению $x^2+3x+1\equiv 0 \pmod{25}$, необходимо, чтобы $x^2+3x+1\equiv 0 \pmod 5$, или $x\equiv 1;\ 6 \pmod{25}$. Однако ни одно из этих значений x не удовлетворяет первому сравнению. Значит, искомых значений не существует.

3) $x=10+15q;\ 5+15q;\ 7+15q;\ 2+15q$, где $q=0;\ 1;\ 2;\ \dots$.

285. 1) $x\equiv 0 \pmod p$; 2) $x\equiv a \pmod 2$.

286. Число классов вычетов, взаимно простых с модулем $p>2$, равно $p-1$.

287. Каждое из сравнений $x^{\frac{p-1}{2}}\equiv 1 \pmod p$ и $x^{\frac{p-1}{2}}\equiv -1 \pmod p$, где $p>2$, имеет $\frac{p-1}{2}$ решений (задача 224).

288. По условию данное сравнение имеет решение $x\equiv x_0 \pmod p$. Тогда, очевидно, оно имеет еще одно решение $x\equiv -x_0 \pmod p$. Более двух решений сравнение второй степени по простому модулю иметь не может.

289. По условию $a^2\equiv 1 \pmod p$, откуда $a\equiv \pm 1 \pmod p$.

290. 1) $(-3)^3=-27\equiv 1 \pmod 7$, поэтому данное сравнение имеет решения. Имеем: $x^2\equiv 4 \pmod 7$, откуда $x\equiv \pm 2 \pmod 7$.

2) $x\equiv \pm 5 \pmod{11}$. 3)—4) Решений нет.

291. 1) Если $a_i^{\frac{p-1}{2}}\equiv 1 \pmod p$, где $i=1;\ 2;\ \ldots,\ n$, то

$$\left(\prod_{i=1}^{n} a_i\right)^{\frac{p-1}{2}}\equiv 1 \pmod p.$$

2) Если $a_i^{\frac{p-1}{2}}\equiv -1 \pmod p$, то $\left(\prod\limits_{i=1}^{n} a_i\right)^{\frac{p-1}{2}}\equiv (-1)^n \pmod p$.

3) Если $a_1^{\frac{p-1}{2}}\equiv 1 \pmod p$ и $a_2^{\frac{p-1}{2}}\equiv -1 \pmod p$, то

$$(a_1a_2)^{\frac{p-1}{2}}\equiv -1 \pmod p.$$

292. 1) $a\equiv 1;\ 4 \pmod 5$; 2) $a\equiv 1;\ 2;\ 4 \pmod 7$; 3) $a\equiv 1;\ 4;\ 3;\ 9;\ 5 \pmod{11}$; 4) $a\equiv 1;\ 4;\ 3;\ 9;\ 12;\ 10 \pmod{13}$.

293. Дано $\frac{p-1}{2}$ несравнимых и взаимно простых с модулем чисел $1;\ 2;\ 3;\ \ldots;\ \frac{p-1}{2}$. Четная степень каждого из них—квадратичный вычет.

294. 1) По критерию Эйлера необходимо и достаточно, чтобы $a^{\frac{3-1}{2}}=a\equiv 1 \pmod 3$.

2) $a^{\frac{5-1}{2}}=a^2\equiv 1 \pmod 5$, откуда $a\equiv \pm 1 \pmod 5$.

3) $a^3\equiv 1 \pmod 7$, откуда $a\equiv 1;\ 2;\ 4 \pmod 7$.

4) $a\equiv 1;\ 3;\ 9;\ 4;\ 5 \pmod{11}$.

295. $(-1)^{\frac{p-1}{2}}\Big|_{p=4n+1}=(-1)^{2n}=1;\ (-1)^{\frac{p-1}{2}}\Big|_{p=4n+3}=$

$$=(-1)^{2n+1}=-1.$$

296. Если $x(x+1)\equiv 1 \pmod{13}$, то $(2x+1)^2\equiv 5 \pmod{13}$, но $\left(\frac{5}{13}\right)=-1$.

297. Данное сравнение равносильно сравнению $(2x+1)^2 \equiv$ $\equiv 4a+1 \pmod{13}$, откуда $4a+1 \equiv 0;\ 1;\ 4;\ 9;\ 16;\ 25;\ 36 \pmod{13}$ (задача 293) и $a \equiv 3;\ 0;\ 4;\ 2;\ 7;\ 6;\ 12 \pmod{13}$.

298. Если $a^2+b^2 \equiv 0 \pmod p$, то при условии $(a, b)=1$ имеем $a \not\equiv 0 \pmod p$ и $b \not\equiv 0 \pmod p$. Пусть x—число целое, удовлетворяющее сравнению $bx \equiv 1 \pmod p$, откуда $(bx)^2 \equiv 1 \pmod p$. Так как $(ax)^2+(bx)^2 \equiv 0 \pmod p$, то $(ax)^2+1 \equiv 0 \pmod p$. Это возможно только при $p=4n+1$ (задача 295).

299. Пусть $p_1;\ p_2;\ \ldots;\ p_k$ — первые k простых чисел вида $4n+1$. Число $(p_1p_2\ldots p_k)^2+1$ делится на простые числа вида $4n+1$ и только на такие простые числа (задача 295). Однако эти делители не совпадают ни с одним из чисел $p_1;\ p_2;\ \ldots;\ p_k$.

300. 1) Необходимо, чтобы $4x^2 \equiv 6 \pmod 5$, откуда $x=\pm 2+5q$. Подстановка в уравнение дает $y=2\pm 16q+20q^2$. 2) $5x^2 \equiv 7 \pmod{11}$, или $x^2 \equiv 8 \pmod{11}$ не имеет решений, поэтому данное уравнение также не имеет решений. 3) $x=8+11q$, $y=-1+6q+11q^2$ и $x=2+11q$, $y=-1-6q+11q^2$. 4) $x=10+13q$, $y=-q+13q^2$ и $x=-2+13q$, $y=12-25q+13q^2$. 5) Решений нет.

301. По условию $a^{\frac{p-1}{2}}=a^{2n+1} \equiv 1 \pmod p$, откуда $a^{2n+2} =$ $=(a^{n+1})^2 \equiv a \pmod p$.

302. При $p=4n+3$ число $\frac{p-1}{2}$ — нечетное и из $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ следует $(-a)^{\frac{p-1}{2}} \equiv -1 \pmod p$, а из $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ следует $(-a)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Если же $p=4n+1$, то число $\frac{p-1}{2}$ — четное и $a^{\frac{p-1}{2}}=(-a)^{\frac{p-1}{2}}$.

303. По условию $a^{\frac{p-1}{2}}=a^{4n+3} \equiv 1 \pmod p$, откуда $a^{4n+4}=$ $=(a^{2n+2})^2 \equiv a \pmod p$ и $x \equiv \pm a^{2n+2} \pmod p$ или $x \equiv \pm a^{\frac{p-1}{4}} \pmod p$.

304. 1) $\left(\frac{5}{p}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right)=\left(\frac{p}{5}\right)$. Следовательно, чтобы $a=5$ было квадратичным вычетом по модулю p, необходимо и достаточно, чтобы $p^{\frac{5-1}{2}}=p^2 \equiv 1 \pmod 5$, откуда $p=\pm 1+5q$. Если же $p=\pm 3+5q$, то $a=5$ — квадратичный невычет. 2) $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)=1$; по модулю же 3 существует один класс квадратичных вычетов: $p\equiv 1 \pmod 3$. 3) $\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$.

Если $p=1+3q$, то $\left(\frac{3}{p}\right)=(-1)^{\frac{3q}{2}}\left(\frac{1}{3}\right)=(-1)^{\frac{3q}{2}}$, откуда $a=3$ является квадратичным вычетом тогда и только тогда, когда $q=4k$ или $p=1+12k$.

Испытание чисел $5+12k$, $7+12k$ и $11+12k$ показывает, что $a=3$ является квадратичным вычетом по простым модулям $1+12k$ и $11+12k$; по простым модулям вида $5+12k$ и $7+12k$ число является квадратичным невычетом.

4) Чтобы $(-1)^{\frac{p^2-1}{8}}=1$, необходимо и достаточно, чтобы $\frac{p^2-1}{8}=2k$ или $p^2\equiv 1 \pmod{16}$, откуда $p=1+2t$ или $p=7+8t$. По простым модулям вида $p=3+8t$ и $p=5+8t$ имеем $\left(\frac{2}{p}\right)=-1$.

5) $\left(\frac{-7}{p}\right)=\left(\frac{p}{7}\right)$; сравнение $x^2\equiv p \pmod 7$ разрешимо при $p\equiv 1;\ 2;\ 4 \pmod 7$ и неразрешимо при $p\equiv 3;\ 5;\ 6 \pmod 7$.

305. 1) Имеем $(2x+1)^2\equiv 5 \pmod p$. Чтобы это сравнение имело решения, необходимо и достаточно, чтобы $\left(\frac{5}{p}\right)=1$ или $\left(\frac{p}{5}\right)=1$, откуда $p\equiv 1;\ 4 \pmod 5$ или $p=1+5n;\ 4+5m$. 2) Имеем $(2x-1)^2\equiv 9 \pmod p$, откуда p—любое нечетное простое число. 3) Имеем $(2x-1)^2\equiv 13 \pmod p$. Условие $\left(\frac{13}{p}\right)=1$ равносильно условию $\left(\frac{p}{13}\right)=1$, откуда $p=13$ и $p\equiv 1;\ 4;\ 9;\ 3;\ 12;\ 10 \pmod{13}$.

306. 1) Если разрешимо либо $x^2\equiv 13 \pmod p$, либо $x^2\equiv 17 \pmod p$, то разрешимо и данное сравнение. При $\left(\frac{13}{p}\right)=\left(\frac{17}{p}\right)=-1$ имеем $\left(\frac{13}{p}\right)\left(\frac{17}{p}\right)=\left(\frac{221}{p}\right)=1$, т. е. данное сравнение опять-таки является разрешимым.

308. 1) $\left(\frac{13}{7}\right)=\left(\frac{-1}{7}\right)=(-1)^3=-1$.

2) $\left(\frac{22}{13}\right)=\left(\frac{-4}{13}\right)=\left(\frac{-1}{13}\right)=(-1)^6=1$.

3) $\left(\frac{426}{491}\right)=\left(\frac{-65}{491}\right)=-\left(\frac{5}{491}\right)\left(\frac{13}{491}\right)=-\left(\frac{491}{5}\right)\left(\frac{491}{13}\right)=-1$.

4) $\left(\frac{37}{67}\right)=\left(\frac{67}{37}\right)=\left(\frac{-7}{37}\right)=\left(\frac{37}{7}\right)=\left(\frac{2}{7}\right)=1$.

309. $\sum\limits_{x=1}^{p-1}\left(\frac{x}{p}\right)=0$, так как число классов квадратичных вычетов равно числу классов квадратичных невычетов. Следовательно, $\sum\limits_{x=2}^{p-1}\left(\frac{x}{p}\right)=-\left(\frac{1}{p}\right)=-1$.

310. $\left(\frac{5}{19}\right)=\left(\frac{5}{29}\right)=1$ и $\left(\frac{2}{97}\right)=\left(\frac{241}{587}\right)=\left(\frac{151}{587}\right)=-1$.

311. $\left(\frac{13}{41}\right)=\left(\frac{41}{13}\right)=-1$.

312. 1) Если $a\equiv b \pmod m$, то $\left(\frac{a}{p_i}\right)=\left(\frac{b}{p_i}\right)$, где $i=1,2,\ldots k$, поэтому $\left(\frac{a}{m}\right)=\Pi\left(\frac{a}{p_i}\right)=\Pi\left(\frac{b}{p_i}\right)=\left(\frac{b}{m}\right)$.

2) $\left(\frac{ab}{m}\right)=\Pi\left(\frac{ab}{p_i}\right)=\Pi\left(\frac{a}{p_i}\right)\cdot\Pi\left(\frac{b}{p_i}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.

3) $\left(\frac{-1}{m}\right)=\Pi\left(\frac{-1}{p_i}\right)=(-1)^{\sum\frac{p_i-1}{2}}$. Так как $\frac{m-1}{2}=$

$$=\frac{\Pi p_i-1}{2}=\frac{\Pi\,[1+(p_i-1)]-1}{2}=\frac{\Sigma(p_i-1)+4q}{2}=$$

$$=\sum\frac{p_i-1}{2}+2q, \text{ то } \left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}.$$

4) Если $m=\prod\limits_{i=1}^{k}p_i$ и $n=\prod\limits_{j=1}^{t}q_j$ — различные нечетные числа (больше единицы) и $(m, n)=1$, то $\left(\frac{n}{m}\right)=\prod\limits_{i=1}^{k}\left(\frac{n}{p_i}\right)=$

$$=\Pi\left(\frac{q_1q_2\ldots q_t}{p_i}\right)=\Pi\left(\frac{q_1}{p_i}\right)\cdot\Pi\left(\frac{q_2}{q_i}\right)\ldots\Pi\left(\frac{q_t}{p_i}\right)=$$

$$=(-1)^{\frac{q_1-1}{2}\cdot\Sigma\frac{p_i-1}{2}}\left(\frac{m}{q_1}\right)\cdot(-1)^{\frac{q_2-1}{2}\cdot\Sigma\frac{p_i-1}{2}}\left(\frac{m}{q_2}\right)\ldots$$

$$\ldots(-1)^{\frac{q_t-1}{2}\cdot\Sigma\frac{p_i-1}{2}}\left(\frac{m}{q_t}\right)=(-1)^{\Sigma\frac{p_i-1}{2}\cdot\Sigma\frac{q_j-1}{2}}\left(\frac{m}{n}\right)=$$

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

313. 1) 2111 — число простое; $\left(\frac{903}{2111}\right)=-\left(\frac{2111}{903}\right)=-\left(\frac{305}{903}\right)=$
$=-\left(\frac{903}{305}\right)=-\left(\frac{-12}{305}\right)=-\left(\frac{-1}{305}\right)\left(\frac{3}{305}\right)=-\left(\frac{305}{3}\right)=-\left(\frac{2}{3}\right)=1.$

2) 383 — число простое и $\left(\frac{219}{383}\right)=1$. 3) $1964=4\cdot 491$; $\left(\frac{7}{491}\right)=-1$ и $x^2\not\equiv 7 \pmod{491}$, следовательно, $x^2\not\equiv 7 \pmod{1964}$.

314. Если $\left(\frac{a}{p}\right)=1$, то $x^2\not\equiv a \pmod p$ и тем более $x^2\not\equiv a \pmod{p^\alpha}$. Если же $\left(\frac{a}{p}\right)=-1$, то существуют значения x, удовлетворяющие уравнению $x^2=a+pq$ $(q=0;\ \pm 1;\ \pm 2;\ \dots)$. Чтобы эти значения x удовлетворяли данному сравнению, необходимо и достаточно, чтобы $a+pq\equiv a \pmod{p^\alpha}$, откуда $q\equiv 0 \pmod{p^{\alpha-1}}$.

315. 1) $\left(\frac{7}{3}\right)=1$, следовательно, решения существуют; $x\equiv\pm 13 \pmod{27}$, 2) $\left(\frac{59}{5}\right)=1$; $x\equiv\pm 53 \pmod{125}$.

316. По определению символа Якоби $\left(\frac{a}{3}\right)\left(\frac{a}{5}\right)=1$, где $\left(\frac{a}{3}\right)$ и $\left(\frac{a}{5}\right)$ — символы Лежандра. Последнее равенство имеет место либо при $\left(\frac{a}{3}\right)=\left(\frac{a}{5}\right)=1$, либо при $\left(\frac{a}{3}\right)=\left(\frac{a}{5}\right)=-1$. При помощи критерия Эйлера эти условия можно записать так:

$$\begin{cases} a\equiv 1 \pmod 3, \\ a^2\equiv 1 \pmod 5 \end{cases} \quad \text{и} \quad \begin{cases} a\equiv -1 \pmod 3, \\ a^2\equiv -1 \pmod 5, \end{cases}$$

откуда $a\equiv 1;\ 2;\ 4;\ 8 \pmod{15}$.

317. Соотношение $d=b^2-4ac$ может быть записано в виде $b^2\equiv d \pmod 4$. При $d\equiv 2;\ 3 \pmod 4$ полученное сравнение неразрешимо.

318. При $\alpha=1$ сравнение разрешимо (задача 306). Если при некотором α данное сравнение имеет решение $x\equiv x_0 \pmod{p^\alpha}$, то существует значение t, при котором $x=x_0+p^\alpha\cdot t$, удовлетворяющее сравнению $x^2\equiv -7 \pmod{p^{\alpha+1}}$. Действительно, $(x_0+p^\alpha\times\times t)^2\equiv -7 \pmod{p^{\alpha+1}}$ равносильно $x_0^2+7+2x_0\,p^\alpha\cdot t+p^{2\alpha}\cdot t^2\equiv\equiv 0 \pmod{p^{\alpha+1}}$; так как $2\alpha\geqslant\alpha+1$ и, следовательно, $p^{2\alpha} ⋮ p^{\alpha+1}$, то имеем

$$\frac{x_0^2+7}{p^\alpha}+2x_0 t\equiv 0 \pmod p, \text{ где } (2x_0,\ p)=1.$$

319. Данное сравнение равносильно системе

$$\begin{cases} x^2 \equiv -11 \pmod 4, \\ x^2 \equiv -11 \pmod p. \end{cases}$$

Исследуем второе сравнение: $\left(\frac{-11}{p}\right) = \left(\frac{p}{11}\right) = \left(\frac{2}{11}\right) = -1.$

320. Требуется исследовать сравнение $\frac{n(n+1)}{2} \equiv 7 \pmod{10}$. При $n=2k$ имеем $k(2k+1) \equiv 7 \pmod{10}$, или

$$\begin{cases} k \equiv 1 \pmod 2, \\ k(2k+1) \equiv 2 \pmod 5. \end{cases}$$

Подставляя из первого сравнения $k = 1+2t$ во второе, после преобразований получаем $t^2 \equiv 3 \pmod 5$. Но последнее сравнение относительно t не имеет решений. Значит, при $n=2k$ данная сумма не оканчивается цифрой 7.

При $n = 2k-1$ также получаем систему сравнений, не имеющую решений. Таким образом, значений n, при которых данная сумма оканчивается цифрой 7, не существует.

321. Сравнение $(m-1)^x \equiv 1 \pmod m$ равносильно сравнению $(-1)^x \equiv 1 \pmod m$. $P_m(m-1) = \begin{cases} 1 \text{ при } m=2, \\ 2 \text{ при } m \geqslant 3. \end{cases}$

322. $a \equiv 3;\ 5;\ 7 \pmod 8$.

323. $P_{11}(2)=10$.

324. Натуральные делители $\varphi(9)$.

325. 1) $P_8(5)=2$, поэтому $x=2n$ ($n=1;\ 2;\ 3;\ \ldots$). 2) x—любое натуральное число, так как $P_3(4)=1$.

326. По условию $a^{2\alpha} \equiv 1 \pmod p$ или $(a^\alpha - 1)(a^\alpha + 1) \equiv 0 \pmod p$, откуда $a^\alpha + 1 \equiv 0 \pmod p$, так как $a^\alpha - 1 \not\equiv 0 \pmod p$.

327. Учесть, что $P_{11}(2) = \varphi(11)$.

328. Если $2^{2^n}+1 \equiv 0 \pmod{p>2}$, то $2^{2^{n+1}} \equiv 1 \pmod p$, откуда $P_p(2) = 2^{n+1}$, так как нечетным показатель не может быть, а при $2^{2^x} \equiv 1 \pmod p$, где $x<n$, имеем $(2^{2^x})^{2^{n-x}} = 2^{2^n} \equiv 1 \pmod p$, что противоречит исходному положению. Таким образом, $p-1 = k \cdot 2^{n+1}$ и $p = k \cdot 2^{n+1} + 1$.

329. Учесть, что $P_m{\underset{a-1}{}}(a) = m$.

330. 1) Необходимо, чтобы $5^x \equiv 1 \pmod 3$ или $(-1)^x \equiv 1 \pmod 3$, откуда $x=2q$ ($q = 1;\ 2;\ \ldots$). Чтобы найти $P_9(5)$, следует рассмотреть соотношение $\varphi(9) : 2q$, откуда либо $q = 1$, либо $q = 3$; так как $5^2 \not\equiv 1 \pmod 9$, то $P_9(5) = 6$. Таким образом, $x = 6n$ ($n=1;\ 2;\ 3;\ \ldots$). 2) $x=20\,n$. 3) $x=14\,n$. 4) $x=21\,n$.

331. $\varphi(\varphi(7))=2$. Так как $P_7(3)=6$, то и $P_7(3^5) = 6$. Искомые классы можно записать: $a \equiv 3;\ 5 \pmod 7$.

332. $a \equiv 5 \pmod 6$.

333. Испытать приведенную систему остатков.

334. 1) $P_9(5)=\varphi(9)=6$, поэтому данное сравнение имеет решение при любом значении b, взаимно простом с модулем. 2) $P_9(4)=3$, поэтому данное сравнение имеет решение лишь при $b\equiv 4;\ 4^2;\ 4^3 \pmod 9$ или $b\equiv 4;\ 7;\ 1 \pmod 9$.

335. $\varphi(m)-P_m(a)$.

336. $P_{11}(2)=P_{11}(2^3)=P_{11}(2^7)=P_{11}(2^9)=10$, откуда $a\equiv 2;\ 8;\ 5;\ 10 \pmod{11}$.

337. Условие $6^x\equiv 1 \pmod{23}$ равносильно $x\cdot \operatorname{ind} 6\equiv 0 \pmod{22}$, или $x\equiv 0 \pmod{11}$, откуда $P_{23}(6)=11$.

339. Условие $a^x\equiv 1 \pmod p$ равносильно $x\cdot\operatorname{ind} a\equiv 0 \pmod{p-1}$. Пусть $(\operatorname{ind} a,\ p-1)=d$, тогда $x\equiv 0\left(\mathrm{mod}\ \dfrac{p-1}{d}\right)$ и $P_p(a)=\dfrac{p-1}{d}$. Теперь ясно, что $P_p(a)=p-1$ тогда и только тогда, когда $d=1$.

340. По модулю 13 взаимно простыми с 12 индексами являются 1, 5, 7 и 11. По таблице индексов им соответствуют числа 10, 6, 11 и 7. Таким образом, $a\equiv 10;\ 6;\ 11;\ 7 \pmod{13}$.

341. 1) $x\equiv 31 \pmod{37}$. 2) $x\equiv 5;\ 6 \pmod{11}$. 3) $x\equiv 27;\ 24;\ 35;\ 22;\ 15 \pmod{41}$. 4) $x\equiv 29;\ 12;\ 21 \pmod{31}$.

342. 1) Чтобы $3a^2\equiv 5 \pmod{17}$, необходимо и достаточно, чтобы $a\equiv 9;\ 8 \pmod{17}$, что можно найти индексированием. 2) $a\equiv 10;\ 13 \pmod{23}$. 3) Искомых значений a не существует.

343. 1) $x=23+66q$ $(q=0;\ 1;\ 2;\ \ldots)$. 2) $x=7+46q$ $(q=0;1;2;\ldots)$. 3) Имеем $3x\cdot\operatorname{ind} 21\equiv 5$, $\operatorname{ind}(21) \pmod{28}$, так как $(\operatorname{ind} 21, 28)=1$ (см. таблицу), то $3x\equiv 5 \pmod{28}$, откуда $x=11+28q$, $q=0;1;2;\ldots$.

344. Известно, что при $a\not\equiv 0$ $(\mathrm{mod}\ p>2)$ имеет место и притом только одно из сравнений $a^{\frac{p-1}{2}}\equiv 1 \pmod p$ и $a^{\frac{p-1}{2}}\equiv -1 \pmod p$. Если $P_p(a)=p-1$, то первое сравнение невозможно.

345. Имеем $n\cdot\operatorname{ind} x\equiv\operatorname{ind} a \pmod{p-1}$, откуда необходимо и достаточно, чтобы $\operatorname{ind} a\equiv 0 \pmod{(n,\ p-1)=d}$. Умножая части последнего сравнения на $\dfrac{p-1}{d}$, получаем $a^{\frac{p-1}{d}}\equiv 1 \pmod p$.

Замечание. При $n=2$ имеем $d=2$, так что полученное соотношение действительно является обобщением критерия Эйлера.

346. 1) $d=1$ и $20^6\equiv(-1)^6\equiv 1 \pmod 7$, поэтому данное сравнение имеет решение; $x\equiv 6 \pmod 7$. 2) $d=2$ и $9^{\frac{10}{2}}\equiv(-2)^5\equiv$ $\equiv 1 \pmod{11}$, поэтому данное сравнение имеет решение; $x\equiv 2;\ 9 \pmod{11}$. 3) Данное сравнение равносильно сравнению $x^8\equiv$ $\equiv 6 \pmod{13}$, которое не имеет решения, так как $d=4$ и $6^{\frac{12}{4}}\equiv$ $\equiv 8 \pmod{13}$. Действительно, данное сравнение приводит к линейному сравнению относительно $\operatorname{ind} x$, не имеющему решений.

347. Индексирование $x^2\equiv a \pmod p$ дает $2\cdot\operatorname{ind} x\equiv$ $\equiv\operatorname{ind} a \pmod{p-1}$, откуда значения $\operatorname{ind} x$ существуют тогда и только тогда, когда $\operatorname{ind} a\equiv 0 \pmod{(2,\ p-1)=2}$.

348. Пусть требуется перейти от системы индексов с основанием a_1 к системе с основанием a_2. Индексирование $a_2^{\operatorname{ind}_{a_2} b} \equiv b \pmod p$ по основанию a_1 дает $\operatorname{ind}_{a_2} b \cdot \operatorname{ind}_{a_1} a_2 \equiv \operatorname{ind}_{a_1} b \pmod{p-1}$, откуда $\operatorname{ind}_{a_2} b \equiv \operatorname{ind}_{a_1} b \cdot (\operatorname{ind}_{a_1} a_2)^{\varphi(p-1)-1} \pmod{p-1}$. Например, в соответствии с тем, что $\operatorname{ind}_2 7 = 7 \pmod{11}$, имеем: $\operatorname{ind}_8 7 \equiv 7 \cdot (\operatorname{ind}_2 8)^{\varphi(10)-1} = 7 \cdot 3^3 \equiv 9 \pmod{10}$, откуда $\operatorname{ind}_8 7 = 9 \pmod{11}$.

349. Если $P_p(a) = p-1$, то $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ невозможно; следовательно, имеет место $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, откуда $x^2 \not\equiv a \pmod p$.

350. Как всякий квадратичный вычет, число вида a^2 удовлетворяет соотношению $(a^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$, откуда $P_p(a^2) \neq p-1$.

351. По условию $a, a^2, \dots, a^{p-1}$ приведенная система вычетов по модулю p, поэтому решение сравнения $x^2 \equiv a^{2n+1} \pmod p$, если оно существует, может быть записано в виде $x \equiv a^i \pmod p$, где $i = 1, 2, \dots, p-1$. Но тогда $a^{2i} \equiv a^{2n+1} \pmod p$, откуда $a^t \equiv 1 \pmod p$, где t—число нечетное. По условию же сравнению $a^x \equiv 1 \pmod p$ удовлетворяют только натуральные числа, кратные $p-1$. Полученное противоречие доказывает теорему.

352. Если $P_p(a_1 a_2) = p-1$, то сравнению $(a_1 a_2)^x \equiv 1 \pmod p$ удовлетворяют лишь четные значения x вида $(p-1)n$, где $n = 1, 2, 3, \dots$. С другой стороны, $(\operatorname{ind}_{a_1}(a_1 a_2), p-1) = (\operatorname{ind}_{a_2}(a_1 a_2), p-1) = 1$, откуда $\operatorname{ind}_{a_1}(a_1 a_2) = 2k+1$, $\operatorname{ind}_{a_2}(a_1 a_2) = 2t+1$ и $a_1^{2k+1} \equiv a_2^{2t+1} \equiv a_1 a_2 \pmod p$ или

$$\left.\begin{aligned} a_1^{2k} &\equiv a_2 \\ a_2^{2t} &\equiv a_1 \end{aligned}\right\} \pmod p,$$

следовательно, $(a_1 a_2)^{2(k+t)-1} \equiv 1 \pmod p$, где $2(k+t)-1$ — число нечетное. Полученное противоречие доказывает теорему.

353. Пусть целое число a таково, что $(a, 2^n) = 1$, т. е. является числом вида $4d \pm 1$. Методом математической индукции нетрудно доказать, что $a^{2^{n-2}} \equiv 1 \pmod{2^n}$, где $n \geqslant 3$. Так как $2^{n-2} = \frac{1}{2}\varphi(2^n)$, то $P_{2^n}(a) \neq \varphi(2^n)$.

354. 1) $2^{15} = 32768 \equiv 8 \pmod{360}$, откуда $2^{60} \equiv 8^4 \equiv 136 \pmod{360}$ и $2^{64} \equiv 136 \cdot 2^4 \equiv 16 \pmod{360}$. Искомый остаток равен 16. 2) $1532^5 - 1 \equiv 2^5 - 1 \equiv 4 \pmod 9$. 3) $(12371^{56} + 34)^{28} \equiv (50^{56} + 34)^{28} \equiv (16+34)^{28} \equiv 70 \pmod{111}$. 4) $4! \equiv 2 \pmod{11}$, откуда $6! \equiv 60 \equiv 5 \pmod{11}$, $7! \equiv 35 \equiv 2 \pmod{11}$ и $8! \equiv 16 \equiv 5 \pmod{11}$. 5) $(a^x, 13) = (2, 13) = 1$, поэтому, разделив почленно второе сравнение на первое, получаем $a \equiv 3 \pmod{13}$.

355. 1) $174^{249} \equiv 5^{249} \pmod{13}$. По теореме Эйлера $5^{12} \equiv 1 \pmod{13}$. Так как $249 = 12 \cdot 20 + 9$, то $5^{249} \equiv 5^9 = (5^4)^2 \cdot 5 \equiv 5 \pmod{13}$.

2) $1863^5 \equiv 3^5 \pmod{10}$; $3^{\varphi(10)} \equiv 1 \pmod{10}$, откуда $3^5 \equiv 3 \pmod{10}$; $1863^5 - 5 \equiv -2 \equiv 8 \pmod{10}$. 3) $2^{\varphi(37)} = 2^{36} \equiv 1 \pmod{37}$, откуда $2^{72} \equiv 1 \pmod{37}$ и $2^{73} \equiv 2 \pmod{37}$; с другой стороны, $2^{\varphi(73)} = 2^{72} \equiv 1 \pmod{73}$ и $2^{73} \equiv 2 \pmod{73}$; таким образом, $2^{73} \equiv 2 \pmod{37\cdot 73}$. Так как $2^9 \equiv 1 \pmod{73}$, то $2^{36} \equiv 1 \pmod{73}$ и $2^{37} \equiv 2 \pmod{73}$; с другой стороны, $2^{37} \equiv 2 \pmod{37}$; следовательно, $2^{37} \equiv 2 \pmod{37\cdot 73}$. Теперь $2^{37\cdot 73} \equiv 2^{73} \equiv 2 \pmod{37\cdot 73}$, откуда $2^{37\cdot 73-1} \equiv 1 \pmod{37\cdot 73}$.

356. 1) 0 и 1. 2) 4 и 9. 3) 8 и 0. 4) 5 и 3. Указание. Найти остатки от деления данных чисел на 100.

357. 3) $102=2\cdot 3\cdot 17$. Так как

$$\left.\begin{aligned} 220 &\equiv 0 \\ 69 &\equiv 1 \\ 119 &\equiv 1 \end{aligned}\right\} \pmod{2},$$

то $M = 220^{119^{69}} + 69^{220^{119}} + 119^{69^{220}} \equiv 2 \equiv 0 \pmod{2}$. Так как

$$\left.\begin{aligned} 220 &\equiv 1 \\ 69 &\equiv 0 \\ 119 &\equiv -1 \end{aligned}\right\} \pmod{3},$$

то $M \equiv 0 \pmod{3}$. Наконец, в силу

$$\left.\begin{aligned} 220 &\equiv -1 \\ 69 &\equiv 1 \\ 119 &\equiv 0 \end{aligned}\right\} \pmod{17}$$

имеем $M \equiv 0 \pmod{17}$. Таким образом, $M \equiv 0 \pmod{102}$. 4) $36 \equiv 5 \pmod{31}$, откуда $6^{2n+1} \equiv 6\cdot 5^n \pmod{31}$. Так как $6 \equiv -25 \pmod{35}$, то $6^{2n+1} \equiv -5^{n+2} \pmod{31}$ или $6^{2n+1} + 5^{n+2} \equiv 0 \pmod{31}$.

358. Обозначим искомый остаток через x $(0 \leqslant x < m)$ и рассмотрим сравнение $4^{\varphi(m)-1} \equiv x \pmod{m}$ или $4^{\varphi(m)} \equiv 4x \pmod{m}$. По теореме Эйлера $4^{\varphi(m)} \equiv 1 \pmod{m}$, поэтому имеем $4x \equiv 1 \pmod{m}$. По модулю 4 нечетные числа имеют вид $4q \pm 1$. Если $m=4q+1$, $q=1, 2, 3, \ldots$, то имеем $4x \equiv 1 + 3m = 12q + 4 \pmod{m}$ или $x \equiv 3q + 1 = \frac{3m+1}{4} \pmod{m}$, где $\frac{3m+1}{4} < m$, и при $m > 1$ служит искомым остатком. Если же $m = 4q - 1$, то из $4x \equiv 1 + m = 4q \pmod{m}$ получаем $x \equiv q = \frac{m+1}{4} \pmod{m}$ и находим, что $\frac{m+1}{4}$ служит искомым остатком.

359. 1) Индексирование сравнения $10^{10} \equiv x \pmod{67}$ дает $\operatorname{ind} x \equiv 28 \pmod{66}$, откуда $x=23$. 2) 3.

360. 1) $10^i \equiv 4 \pmod{6}$, где $i = 1, 2, 3, \ldots$, следовательно, $N \equiv 4\,((a_n + \ldots + a_2 + a_1) + a_0) \pmod{6}$, т. е. $N \vdots 6$ тогда и только тогда, когда на 6 делится число вида $4\,(a_n + \ldots + a_2 + a_1) + a_0$. Например, $26676 \vdots 6$, так как $4\cdot 21 + 6 = 90 \vdots 6$, но 2590 не $\vdots 6$, так как $4\cdot 16 = 64$ не $\vdots 6$.

2) $\left.\begin{array}{l} 10 \equiv 2 \\ 10^2 \equiv 4 \\ 10^i \equiv 0, \; i=3, 4, \ldots \end{array}\right\}$ (mod 8),

поэтому $N \equiv 4a_2 + 2a_1 + a_0$ (mod 8), и, следовательно, чтобы $N \equiv 0$ (mod 8), необходимо и достаточно, чтобы $\overline{4a_2 + 2a_1 + a_0} \equiv 0$ (mod 8). 3) $N \equiv 4\,(a_n + \ldots + a_3 + a_2) + \overline{a_1 a_0}$ (mod 12). Например, $19641964 \equiv 4\;(196 + 4 + 1 + 9) + 64 = 184 \equiv 4 + 84 = 88 \not\equiv$ $\not\equiv 0$ (mod 12), т. е. $19641964 \not\equiv 0$ (mod 12). 4) $N \equiv 10\,(a_n + \ldots + a_2 +$ $+ a_1) + a_0$ (mod 15; 18; 45).

Замечание. Другие модули, допускающие данный признак делимости, могут быть найдены как делители разности $10^x - 10 = 10\,(10^{x-1} - 1) = 10.\,99\ldots 9$, где второй сомножитель содержит $x-1$ цифр.

361. Число делится на 11 тогда и только тогда, когда разность между суммой его цифр, стоящих на нечетных местах, и суммой остальных цифр делится на 11.

362. Представить данное число в системе счисления с основанием 1000 и применить признак, аналогичный признаку делимости на 11 в десятичной системе счисления.

363. Представить число в системе счисления с основанием 1000 и применить признак Паскаля.

364. Так как $10xa_0 \equiv a_0$ (mod m), то

$$N \equiv 10\,(\overline{a_n \ldots a_2 a_1} + a_0 x) (\mathrm{mod}\; m),$$

откуда и вытекает справедливость сформулированного в задаче признака делимости.

365. 1) Сравнение $10x \equiv 1$ (mod 19) имеет решение $x \equiv$ $\equiv 2$(mod 19). Последовательное применение теоремы предыдущей задачи видно из следующей записи:

$$\begin{array}{r} 185231 \\ +\quad 2 \\ \hline 18525 \\ +\quad 10 \\ \hline 1862 \\ +\quad 4 \\ \hline 190 \end{array} \;\vdots\; 19,$$

значит, и $185\,231 \,\vdots\, 19$.

3) Решение сравнения $10x \equiv 1$ (mod 7) может быть записано в виде $x \equiv -2$ (mod 7). Если воспользоваться вычетом $x = -2$, то

$$\begin{array}{r} 192843 \\ -\quad 6 \\ \hline 19278 \\ -\quad 16 \\ \hline 1911 \\ -\quad 2 \\ \hline 189 \\ -\quad 18 \\ \hline 0 \end{array} \;\vdots\; 7,$$

значит, и $192\,843 \,\vdots\, 7$.

366. Пусть $A = |x| \cdot q + r$, $0 \leq r < |x|$. Тогда $N = 10(|x|q + r) + a_0 = 10 \cdot |x| \cdot q + \overline{ra_0} \equiv$

$$\equiv \begin{cases} q + \overline{ra_0} \pmod m \text{ при } x > 0, \\ -q + \overline{ra_0} \pmod m \text{ при } x < 0. \end{cases}$$

Например, $2772 \equiv 0 \pmod{21}$, так как при $x = -2$ и $277 = 2 \cdot 138 + 1$ имеем $-138 + 12 = -126 \equiv 0 \pmod{21}$.

367. Имеем

$$\begin{cases} \overline{13\,xy\,45z} \equiv 0 \pmod 8, \\ \overline{13\,xy\,45z} \equiv 0 \pmod 9, \\ \overline{13\,xy\,45z} \equiv 0 \pmod{11}. \end{cases}$$

По признаку деления на 8 имеем $\overline{45z} = 450 + z \equiv 0 \pmod 8$, откуда $z = 6$. При $z = 6$ по признакам делимости на 9 и на 11 имеем

$$\begin{cases} x + y + 1 \equiv 0 \pmod 9, \\ x - y + 3 \equiv 0 \pmod{11}, \end{cases}$$

откуда $x = 8$ и $y = 0$. Ответ: 1380456.

368. Сравнение $N = a_n g^n + \ldots + a_2 g^2 + a_1 g + a_0 \equiv a_n + \ldots + a_1 + a_0 \pmod 2$ равносильно сравнению $a_n(g^n - 1) + \ldots + a_2(g^2 - 1) + a_1(g - 1) \equiv 0 \pmod 2$, которое имеет место независимо от a_i тогда и только тогда, когда $g - 1 \equiv 0 \pmod 2$ или $g = 1 + 2q$, $q = 1, 2, \ldots$. Таким образом, чтобы указанный признак делимости имел место, необходимо и достаточно, чтобы основание системы счисления было нечетным. В случае произвольного модуля $m > 1$ получаем: $g = 1 + mq$, $q = 1, 2, \ldots$.

369. На основании первого условия для искомого основания системы счисления имеем $g = 5x + 1$, $x = 1, 2, \ldots$ (задача 368). Пусть делимое есть $N = (\overline{a_n \ldots a_3 a_2 a_1 a_0})_g$, тогда второе условие можно записать: $N \equiv \overline{a_1 a_0} \pmod 7$ или $a_n g^n + \ldots + a_3 g^3 + a_2 g^2 \equiv 0 \pmod 7$, откуда $g \equiv 0 \pmod 7$ или $g = 7y$, $y = 1, 2, \ldots$. Таким образом, $7y = 5x + 1$ или $7y \equiv 1 \pmod 5$, откуда $y = 3 + 5q$, $q = 0, 1, 2, \ldots$, $g = 21 + 35q$ и $\min q = 21$.

370. 1) 5. 2) 6. 3) 21. 4) 96. Последние два примера целесообразно решать при помощи индексов.

371. 1) 6. 2) 2.

372. 11, 33 и 99 — делители 99, не делящие 9.

373. 1) Сравнение $10^x \equiv 1 \pmod{17 \cdot 23}$ равносильно системе

$$\begin{cases} 10^x \equiv 1 \pmod{17}, \\ 10^x \equiv 1 \pmod{23}. \end{cases}$$

Решая каждое сравнение этой системы индексированием, получаем

$$\begin{cases} x \equiv 0 \pmod{16}, \\ x \equiv 0 \pmod{22}, \end{cases}$$

откуда $x \equiv 0 \pmod{176}$ и $P_{17 \cdot 23}(10) = 176$.

2) $P_{53 \cdot 59}(10) = 754$.

374. Сравнение $10^x \equiv 1 \pmod{p_1 p_2}$ равносильно системе

$$\begin{cases} 10^x \equiv 1 \pmod{p_1}, \\ 10^x \equiv 1 \pmod{p_2} \end{cases} \text{ или } \begin{cases} x \cdot \operatorname{ind}_{p_1} 10 \equiv 0 \pmod{p_1 - 1}, \\ x \cdot \operatorname{ind}_{p_2} 10 \equiv 0 \pmod{p_2 - 1}, \end{cases}$$

или

$$\begin{cases} x \equiv 0 \left(\mathrm{mod}\, \dfrac{p_1-1}{d_1}\right), \\ x \equiv 0 \left(\mathrm{mod}\, \dfrac{p_2-1}{d_2}\right), \end{cases}$$

откуда $x \equiv 0 \left(\mathrm{mod}\left[\dfrac{p_1-1}{d_1}, \dfrac{p_2-1}{d_2}\right]\right)$ и $P_{p_1p_2}(10) = \left[\dfrac{p_1-1}{d_1}, \dfrac{p_2-1}{d_2}\right]$.

375. 1) $s\,(4237) \cdot s\,(27925) = 16 \cdot 25 \equiv 7 \cdot 7 \equiv 4 \pmod 9$, так как $s\,(118275855) \equiv 6 \pmod 9$. 2) $s\,(42981) = 24 \equiv 6 \pmod 9$, тогда как $s\,(8264) \cdot s\,(5201) = 20 \cdot 8 \equiv 7 \pmod 9$. 3) $2 \cdot s\,(1965) = 2 \cdot 21 \equiv 6 \pmod 9$, тогда как $s\,(3761225) = 26 \equiv 8 \pmod 9$.

377. Если $\sqrt[n]{m} = k$, т. е. $m = k^n$, и s_m, s_k — суммы цифр соответствующих чисел m и k, то $s_m \equiv s_k^n \pmod 9$. Так как $25 \not\equiv 5^5$ $\pmod 9$, то $\sqrt[5]{371293} \neq 23$.

378. (2, 2, 3, 1, 5), (0, 1, 2, 5, 2) и (1, 4, 2, 1, 7).

379. $\dfrac{71}{41}$, $\dfrac{157}{225}$, $\dfrac{539}{103}$, $\dfrac{a^5+4a^3+3a}{a^4+3a^2}$ и $\dfrac{a^3b^2+4a^2b+3a}{a^2b^2+3ab+1}$.

380. 1) $x = \left[\dfrac{73}{30}\right] = 2$. 2) Данное уравнение может быть представлено в виде $(x, y, z) = (1, 2, 3)$, откуда $x = 1$, $y = 2$ $z = 3$.

381. $(1, \overline{2})$, $(2, \overline{1, 1, 1, 4})$ и $(3, \overline{4, 1})$.

382. $(0, \overline{1, 4, 1, 1})$ и $(2, \overline{4, 1})$.

383. Пусть $(2, 2, \ldots, 2) = \alpha_n$, где n — число неполных частных. Если $n = 2k$, то $\alpha_2 = (2,2) = 2 + \dfrac{1}{2}$ и $\alpha_2 : 2 = 1 + \dfrac{1}{4} = (1, 4)$; $\alpha_4 = (2, 2, \alpha_2) = 2 + \dfrac{1}{2 + \dfrac{1}{\alpha_2}}$ и $\alpha_4 : 2 = 1 + \dfrac{1}{4 + \dfrac{1}{\alpha_2 : 2}} = (1, 4, 1, 4)$. Если при некотором k имеем

$$\alpha_{2k} : 2 = (1, 4, 1, 4, \ldots, 1, 4),$$

где $2k$ неполных частных, то

$$\alpha_{2(k+1)} : 2 = \frac{(2, 2, \alpha_{2k})}{2} = 1 + \frac{1}{4 + \dfrac{1}{\alpha_{2k} : 2}} = (1, 4, 1, 4, \ldots, 1, 4),$$

где $2(k+1)$ неполных частных. Итак, $\alpha_{2k} : 2 = (1, 4, 1, 4, \ldots, 1, 4)$, где $2k$ неполных частных, для любого натурального k. Аналогично методом математической индукции доказывается, что $\alpha_{2k+1} : 2 = (1, 4, 1, 4, \ldots, 1, 4, 1, 5)$, где $2k$ неполных частных и $\alpha_3 : 2 = (1,5)$.

Замечание. Вообще, если $\alpha_n = (a, a, \ldots, a)$, где $a > 1$, то $\alpha_{2k} : a = (1, a^2, 1, a^2, \ldots, 1, a^2)$ и $\alpha_{2k+1} : a = (1, a^2, \ldots, 1, a^2, 1, a^2 + 1)$, где в обоих случаях $2k$ неполных частных и во втором случае $\alpha_3 : a = (1, a^2 + 1)$.

384. Применить формулы $P_k = P_{k-1} q_k + P_{k-2}$ и $Q_k = Q_{k-1} q_k + Q_{k-2}$ при $k = n + 2$ и затем при $k = n + 1$.

385. $$\frac{P_n}{P_{n-1}} = \frac{P_{n-1} q_n + P_{n-2}}{P_{n-1}} = q_n + \frac{1}{\dfrac{P_{n-1}}{P_{n-2}}}, \quad \frac{P_{n-1}}{P_{n-2}} = q_{n-1} + \frac{1}{\dfrac{P_{n-2}}{P_{n-3}}}, \ \ldots, \ \frac{P_1}{P_0} = \frac{q_1 q_0 + 1}{q_0} = q_1 + \frac{1}{q_0},$$ откуда $\dfrac{P_n}{P_{n-1}} = (q_n, q_{n-1}, \ldots, q_1, q_0)$. Аналогичный алгоритм имеем и для $\dfrac{Q_n}{Q_{n-1}}$.

386. Если $(P_n, P_{n-1}) = d$, то из $P_n = P_{n-1} q_n + P_{n-2}$ следует, что и $(P_{n-1}, P_{n-2}) = d$. При $n = 2$ имеем $d = (P_1, P_0) = (q_1 q_0 + 1, q_0) = 1$. Утверждение $(Q_n, Q_{n-1}) = 1$ доказывается аналогично.

387. При $n = 1$ имеем верное равенство $2 = \dfrac{(1+\sqrt{2})^2 - (1-\sqrt{2})^2}{(1+\sqrt{2}) - (1-\sqrt{2})}$.

Допустим, что исходное равенство верно для некоторого n. Тогда, обозначая его левую часть через α_n, имеем:

$$\alpha_{n+1} = (2, \alpha_n) = 2 + \frac{1}{\alpha_n} = 2 + \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{(1+\sqrt{2})^{n+1} - (1-\sqrt{2})^{n+1}} =$$

$$= \frac{2(1+\sqrt{2})^{n+1} + (1+\sqrt{2})^n - 2(1-\sqrt{2})^{n+1} - (1-\sqrt{2})^n}{(1+\sqrt{2})^{n+1} - (1-\sqrt{2})^{n+1}} =$$

$$= \frac{(1+\sqrt{2})^n (2+2\sqrt{2}+1) - (1-\sqrt{2})^n (2-2\sqrt{2}+1)}{(1+\sqrt{2})^n - (1-\sqrt{2})^n} =$$

$$= \frac{(1+\sqrt{2})^{n+2} - (1-\sqrt{2})^{n+2}}{(1+\sqrt{2})^{n+1} - (1-\sqrt{2})^{n+1}}.$$

388. 1) $\dfrac{3587}{2743} = (1, 3, 4) = \dfrac{17}{13}$. 2) $\dfrac{1043}{3427} = (0, 3, 3, 2) = \dfrac{7}{23}$.

3) $\dfrac{1491}{2247} = (0, 1, 1, 1, 35) = \dfrac{71}{107}$.

389. $\frac{a^4+3a^2+1}{a^3+2a}=(a,\ a,\ a,\ a)$; свертывание полученной непрерывной дроби приводит к исходной обыкновенной дроби.

390. $\frac{P_n}{P_{n-1}}=(q_n,\ \ldots,\ q_1,\ q_0)=(q_0,\ q_1,\ \ldots,\ q_n)=\frac{P_n}{Q_n}$. В силу несократимости дробей $\frac{P_n}{P_{n-1}}$ (задача 386) и $\frac{P_n}{Q_n}$ из их равенства следует $P_{n-1}=Q_n$.

391. Теорема может быть доказана методом математической индукции при помощи соотношения $Q_n=Q_{n-1}q_n+Q_{n-2}\geqslant 2Q_{n-2}$.

а) При $n=2$ имеем $Q_2\geqslant 2Q_0=2>\sqrt{2}=2^{\frac{2-1}{2}}$. б) Если $Q_k\geqslant 2^{\frac{k-1}{2}}$ для всех $2\leqslant k<n$, то $Q_n\geqslant 2Q_{n-2}\geqslant 2\cdot 2^{\frac{(n-2)-1}{2}}=2^{\frac{n-1}{2}}$.

392. Разложив $\frac{m}{a}$ в непрерывную дробь $(q_0,\ q_1,\ldots,\ q_n)$ и найдя, что $m=P_n$ и $a=Q_n$, имеем указанное соотношение в виде $mQ_{n-1}-aP_{n-1}=(-1)^{n-1}$ или $aP_{n-1}=(-1)^n+mQ_{n-1}$, или $a[(-1)^n bP_{n-1}]\equiv b \pmod m$, откуда $x\equiv(-1)^n bP_{n-1}$ mod m).

393. 1) $\frac{308}{95}=(3,\ 4,\ 7,\ 1,\ 2)$, откуда $n=4$, $P_3=107$ и $x\equiv$ $\equiv 59\cdot 107\equiv 153 \pmod{308}$. 2) $x\equiv -29 \pmod{132}$.

394. Считая $a>0$, $b>0$ и $(a,\ b)=1$, разлагаем $\frac{a}{b}$ в непрерывную дробь. Затем указанное соотношение записываем в виде $aQ_{n-1}-bP_{n-1}=(-1)^{n-1}$, откуда $a\left[(-1)^{n-1}c\cdot Q_{n-1}\right]+b[(-1)^n\times$ $\times c\cdot P_{n-1}\big]=c$. Таким образом, $x_0=(-1)^{n-1}c\cdot Q_{n-1}$ и $y_0=(-1)^n c\times$ $\times P_{n-1}$. Общее решение может быть записано в виде $x=x_0+bt$, $(y=y_0-at$ $(t=0,\pm 1,\pm 2,\ldots)$.

395. 1) $\frac{70}{33}=(2,\ 8,\ 4)$, откуда $n=2$, $\frac{P_1}{Q_1}=\frac{17}{8}$ и $x=-8+$ $+33t$, $y=17-70t$. 2) Представив уравнение в виде $60x+91(-y)=2$, имеем: $\frac{60}{91}=(0,\ 1,\ 1,\ 1,\ 14,\ 2)$, откуда $n=5$, $\frac{P_4}{Q_4}=\frac{29}{44}$ и $x=88+$ $+91t$, $y=-58-60t$ или $x=88+91t$, $y=58+60t$. 3) $x=1270+$ $+359t$, $y=-2020-571t$.

396. 1) $\frac{587}{103}=(5,\ 1,\ 2,\ 3,\ 10)\approx 5{,}7\,(+0{,}0002)$. Приведенная погрешность несколько грубее, чем $\frac{1}{Q_3Q_4}$, но удобнее и пригодна для

обычной практики. 2) $3{,}14159=3+\frac{1}{\frac{100000}{14159}}=3+\frac{1}{(7,15,1,25,1,7,4)}=$
$=(3, 7, 15, 1, 25, 1, 7,$ 4) $\approx \frac{355}{113}(+0{,}000004)$. 3) $\frac{2}{3}(+0{,}07)$.
4) $\frac{2}{37}(+0{,}00005)$.

397. $\frac{355}{113}=(3, 7, 16)$, откуда $\frac{P_1}{Q_1}=\frac{22}{7}$ и $\frac{22}{7}-\frac{355}{113}=\frac{1}{791}=$
$=\frac{2}{1582}<0{,}002$. Ответ: 22 и 7.

398. $\frac{1261}{881}=(1, 2, 3, 7, 8, 2)$. Чтобы удовлетворить заданной мере точности, достаточно иметь $Q_n>\sqrt{\frac{1}{0{,}0001}}=100$. Первой подходящей дробью со знаменателем, большим 100, является $\frac{P_4}{Q_4}=\frac{594}{415}$. Следовательно, $\frac{1261}{884}\approx\frac{594}{415}(-0{,}0001)$. Однако $\frac{P_3}{Q_3}-$
$-\frac{1261}{884}<\frac{1}{51.415}<0{,}0001$, поэтому при заданной мере точности наилучшим приближением данного числа является $\frac{P_3}{Q_3}=\frac{73}{51}$ (легко видеть, что $\frac{1261}{881}-\frac{P_2}{Q_2}>0{,}0001$).

399. 1) $\sqrt{2}=(1, \overline{2})$. Условию $Q_n>\sqrt{\frac{1}{0{,}001}}=31,\ldots$ удовлетворяет $\frac{P_5}{Q_5}=\frac{99}{70}$, т. е. $\sqrt{2}\approx\frac{99}{70}(+0{,}001)$. Но $\sqrt{2}-\frac{P_4}{Q_4}<$
$<\frac{1}{29\cdot 70}<0{,}001$), поэтому наилучшим приближением $\sqrt{2}$ с точностью до 0,001 является $\frac{P_4}{Q_4}=\frac{41}{29}$ (проверить, что $\frac{P_3}{Q_3}-\sqrt{2}>$
$>0{,}001$). 2) $\frac{63}{11}(-0{,}001)$.

400. 1) $x_1=\frac{5+\sqrt{17}}{2}\approx\frac{593}{130}(-0{,}0001)$ и $x_2\approx\frac{57}{130}(+0{,}0001)$.

2) $|x_1|=\frac{5-\sqrt{2}}{2}=(1, 1, 3, \overline{1, 4})\approx\frac{251}{125}(-0{,}0001)$, откуда $x_1\approx-$
$-\frac{251}{125}(+0{,}0001)$; $|x_2|=\frac{5+\sqrt{2}}{2}=(3, \overline{4, 1})\approx\frac{449}{140}(+0{,}0001)$, откуда
$x_2\approx-\frac{449}{140}(-0{,}0001)$.

401. Знак разности $\alpha - \frac{P_n+P_{n+1}}{Q_n+Q_{n+1}} = \frac{P_{n+1}q_{n+2}+P_n}{Q_{n+1}q_{n+2}+Q_n} - \frac{P_n+P_{n+1}}{Q_n+Q_{n+1}} = \frac{(-1)^n(q_{n+2}-1)}{(Q_{n+1}q_{n+2}+Q_n)(Q_n+Q_{n+1})}$ зависит только от четности n, причем при $n=2k$ имеем $\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}} < \alpha$ и при $n=2k+1$ имеем $\alpha < \frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}$. Легко также убедиться в том, что дробь $\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}}$ лежит между $\frac{P_n}{Q_n}$ и α. В соответствии с этим $\left|\alpha - \frac{P_n}{Q_n}\right| > \left|\frac{P_n+P_{n+1}}{Q_n+Q_{n+1}} - \frac{P_n}{Q_n}\right| = \frac{1}{Q_n(Q_n+Q_{n+1})}$.

Замечание. Установленное неравенство дает нижнюю границу для $\left|\alpha - \frac{P_n}{Q_n}\right|$ и, таким образом, дополняет известное неравенство

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

402. Подходящая дробь четного порядка увеличится, а нечетного — уменьшится, так как

$$\frac{P_{n-1}(q_n+m)+P_{n-2}}{Q_{n-1}(q_n+m)+Q_{n-2}} - \frac{P_{n-1}q_n+P_{n-2}}{Q_{n-1}q_n+Q_{n-2}} = \frac{(-1)^{n-2}\cdot m}{A},$$

где $A > 0$ — произведение знаменателей рассматриваемых подходящих дробей.

403. Справедливость утверждения вытекает из того, что $\left|\alpha - \frac{P_n}{Q_n}\right| + \left|\alpha - \frac{P_{n-1}}{Q_{n-1}}\right| = \left|\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right| = \frac{1}{Q_nQ_{n-1}} < \frac{1}{2Q_n^2} + \frac{1}{2Q_{n-1}^2}$. При этом $\left|\alpha - \frac{P_{n-1}}{Q_{n-1}}\right|$ может быть меньше именно $\frac{1}{2Q_{n-1}^2}$, так как $\left|\alpha - \frac{P_{n-1}}{Q_{n-1}}\right| > \frac{1}{Q_{n-1}(Q_{n-1}+Q_n)}$ (задача 401), откуда тем более $\left|\alpha - \frac{P_{n-1}}{Q_{n-1}}\right| > \frac{1}{2Q_n^2}$.

404. 1) $1+\sqrt{1,(6)}$. 2) $\frac{9+\sqrt{221}}{14}$. 3) $\frac{55+\sqrt{380}}{23}$. 4) $\frac{38-\sqrt{5}}{11}$. 5) $\frac{10-\sqrt{2}}{14}$. 6) $\sqrt{a^2+2}$.

405. 1) $\alpha = \dfrac{10\sqrt{2}+P_{k-1}}{3\sqrt{2}+Q_{k-1}}$; $\dfrac{P_k}{Q_k} = (3, 3)$, $\dfrac{P_{k-1}}{Q_{k-1}} = \dfrac{3}{1}$; $\alpha = \dfrac{10\sqrt{2}+3}{3\sqrt{2}+1} = \dfrac{57-\sqrt{2}}{17}$. 2) $\alpha = (2, 1, 5, \overline{2, 1}) = \dfrac{51+4\sqrt{3}}{23}$.

406. Если $x = (a, a, a, \ldots) = (a, x)$, то $x = \dfrac{a+\sqrt{a^2+4}}{2}$. Например, при $a = 2$ имеем $1+\sqrt{2} = (2, 2, 2, \ldots)$, при $a = 3$ имеем $\dfrac{3+\sqrt{13}}{2} = (\overline{3})$ и т. д.

407. 1) $\sqrt{x^2+1} = x + \sqrt{x^2+1} - x = x + \dfrac{1}{x+\sqrt{x^2-1}} = x + \cfrac{1}{2x+\cfrac{1}{2x+\ldots}} = (x, \overline{2x})$. Например, $\sqrt{2} = (1, \overline{2})$, $\sqrt{5} = (2, \overline{4})$, $\sqrt{10} = (3, \overline{6})$ и т. д. 2) $\sqrt{a^4+2a} = a^2 + \sqrt{a^4+2a} - a^2 = a^2 + \cfrac{1}{\cfrac{\sqrt{a^4+2a}+a^2}{2a}}$, $\dfrac{\sqrt{a^4+2a}+a^2}{2a} = \dfrac{2a^2+\sqrt{a^4+2a}-a^2}{2a} = a + \dfrac{1}{\sqrt{a^4+2a}+a^2}$, $\sqrt{a^4+2a}+a^2 = 2a^2 + \sqrt{a^4+2a} - a^2$ и т. д. Таким образом, $\sqrt{a^4+2a} = (a^2, \overline{a, 2a^2})$.

408. $\dfrac{ab+\sqrt{a^2b^2+4ab}}{2b} = (\overline{a, b})$.

409. Речь идет об уравнении $bx^2 - abx - a = 0$ (задача 408), сумма корней которого равна a, откуда $x_2 = a - (\overline{a, b}) = -\dfrac{1}{(\overline{b, a})}$.

410. $\alpha = (\overline{a_0, a_1, \ldots, a_n})$ служит корнем непрерывной функции $f(x) = Q_n x^2 + (Q_{n-1} - P_n)x - P_{n-1}$, вторым корнем которой служит сопряженная иррациональность. Так как $f(0) = -P_{n-1} < 0$ и $f(-1) = P_n - P_{n-1} > 0$, то второй корень $f(x)$ принадлежит интервалу $(-1; 0)$.

411. Так как $x = (a, \overline{b, c}) = a + \dfrac{1}{(\overline{b, c})}$, то $(\overline{b, c}) = \dfrac{1}{x-a}$. Но число $(\overline{b, c})$ служит корнем уравнения $cx^2 - bcx - b = 0$ (задача 409). Следовательно, второй корень этого уравнения можно найти из условия $\dfrac{1}{x-a} = -\dfrac{1}{(\overline{c, b})}$, откуда $x = a - (\overline{c, b})$.

412. $(\overline{a, b})$ удовлетворяет уравнению $bx^2 - abx - a = 0$, вторым корнем которого служит $-\dfrac{1}{(\overline{b, a})} = -(0, \overline{b, a})$ (задачи 408 и 409), откуда $(\overline{a, b})\,(0, \overline{b, a}) = \dfrac{a}{b}$.

413. $\frac{\alpha}{\beta}=\frac{ab+1}{bc+1}$. Числа x и y удовлетворяют соответственно уравнениям $(bc+1)x^2-(abc+a+c-b)x-(ab+1)=0$, $(ab+1)y^2-$ $-(abc+a+c-b)y-(bc+1)=0$, откуда $\frac{x}{y}=\frac{ab+1}{bc+1}$ и, следовательно, $\frac{\alpha}{\beta}=\frac{x}{y}$.

414. Если $\sqrt{m}=(q_0, q_1, q_2, \ldots)$, то $q_0+\sqrt{m}=(2q_0, q_1, q_2, \ldots)>1$ и $-1<q_0-\sqrt{m}<0$. Следовательно, $q_0+\sqrt{m}$ выражается чистой периодической непрерывной дробью, т. е. $q_0+\sqrt{m}=(\overline{2q_0, q_1, q_2, \ldots, q_n})$. Но тогда $\sqrt{m}=(q_0, \overline{q_1, q_2, \ldots, q_n, 2q_0})$, что требовалось доказать. Например, $\sqrt{2}=(1, \overline{2})$, $\sqrt{8}=(2, \overline{1, 4})$, $\sqrt{53}=(7, \overline{3, 1, 1, 3, 14})$ и т. д.

415. 1) Если $\sqrt[4]{4-\sqrt[3]{2}}=x$, то $x^4=4-\sqrt[3]{2}$, откуда $(x^4-4)^3=-2$ или $x^{12}-12x^8+48x^4+66=0$. 2) Данное число удовлетворяет уравнению $x^6-6x^4-6x^3+12x^2-36x+1=0$. 3) Из $a+\sqrt[n]{b}=x$ следует $(x-a)^n=b$, откуда видно, что $a+\sqrt[n]{b}$ является числом алгебраическим. 4) Если $a+i\sqrt{b}=z$, то $(z-a)^2=-b$. 5) Полагая $\cos\frac{\pi}{n}+i\sin\frac{\pi}{n}=z$, имеем $z^n=\cos\pi+i\sin\pi=-1$ или $z^n+1=0$. 6) С помощью соотношения $\sin 3\varphi=3\sin\varphi-4\sin^3\varphi$ можно убедиться, что $\sin 10^\circ$ является корнем многочлена $8x^3-6x+1$.

416. 1) Число $a+bi$ является корнем многочлена $z^2-2az+a^2+b^2$ и не является корнем никакого многочлена первой степени с целыми коэффициентами (последнее легко доказывается рассуждением от противного). Таким образом, $a+bi$ — алгебраическое число второго порядка. 2) $\sqrt[3]{3}$ является корнем двучлена x^3-3 и не является корнем никакого многочлена второй степени x^2+px+q с рациональными коэффициентами; если $\sqrt[3]{9}+p\sqrt[3]{3}+q=0$, то $(\sqrt[3]{9}+p\sqrt[3]{3})^2=q^2$ или $3\sqrt[3]{3}+$ $+6p+p^2\sqrt[3]{9}=q^2$, откуда $3\sqrt[3]{3}+6p+p^2(-p\sqrt[3]{3}-q)=q^2$ или $(3-p^3)\sqrt[3]{3}=$ $=q^2+p^2q-6p$, что невозможно, так как при $3-p^3\neq 0$ имеем $\sqrt[3]{3}=$ $=\frac{q^2+p^2q-6p}{3-p^3}$ — число рациональное. Таким образом, $\sqrt[3]{3}$ — алгебраическое число третьего порядка. 3) $\sqrt[3]{2}-1$ является корнем многочлена $x^3+3x^2+3x-1=0$ и не является корнем никакого многочлена второй степени x^2+px+q с рациональными коэффициентами; если $(\sqrt[3]{2}-1)^2+p(\sqrt[3]{2}-1)+q=0$ или $\sqrt[3]{4}+(p-2)\sqrt[3]{2}=p-q-1$, то $[\sqrt[3]{4}+$ $+(p-2)\sqrt[3]{2}]^2=(p-q-1)^2$ или $(p-2)^2\sqrt[3]{4}+2\sqrt[3]{2}=(p-q-1)^2-4(p-2)$, откуда $(p-2)^2[p-q-1-(p-2)\sqrt[3]{2}]+2\sqrt[3]{2}=(p-q-1)^2-4(p-2)$ или $[(p-2)^3-2]\sqrt[3]{2}=(p-2)^2\ (p-q-1)-(p-q-1)^2+4(p-2)$, что невозможно, так как при $(p-2)^3-2\neq 0$ имеем $\sqrt[3]{2}=\frac{(p-2)^2(p-q-1)}{(p-2)^3-2}-$

$-\dfrac{(p-q-1)^2}{(p-2)^3-2}$ является числом рациональным (?!). Таким образом, $\sqrt[3]{2}-1$ — число алгебраическое третьего порядка. 4) Число $\sqrt{2}-\sqrt{3}$ является корнем многочлена x^4-10x^2+1 и не является корнем никакого кубического многочлена x^3+ax^2+bx+c с рациональными коэффициентами; если $(\sqrt{2}-\sqrt{3})^3+a(\sqrt{2}-\sqrt{3})^2+b(\sqrt{2}-\sqrt{3})+c=0$, то $(b+11)\sqrt{2}-(b+9)\sqrt{3}-2a\sqrt{6}=-5a-c$, что невозможно.

417. а) Корни данного уравнения удовлетворяют уравнению $(x^3+2\sqrt{2}\cdot x^2+2)(x^3+2-2\sqrt{2}\cdot x)=0$ или $(x^3+2)^2-8x^4=0$. б) Корни данного уравнения удовлетворяют уравнению $x^4+24x^2+100=0$.

418. По признаку Эйзенштейна (высшая алгебра) многочлен $x^5-3x^2+12x-6$ неприводим в поле рациональных чисел: все его целые коэффициенты, кроме коэффициента старшего члена, делятся на простое число 3, причем свободный член не делится на 3^2.

419. По Лиувиллю трансцендентным числом является всякая бесконечная непрерывная дробь $\alpha=(q_0, q_1, q_2, \ldots)$, у которой $q_i > (Q_{i-1})^{i-1}$, $i=k$, $k+1$, ... и q_i, $i=0, 1, \ldots, k$ произвольны. Так, при $k=2$ и $q_0=0$, $q_1=1$ имеем: $q_2>Q_1=1$, например, $q_2=2$; тогда $q_3>Q_2^2=(Q_1q_2+Q_0)^2=9$, например, $q_3=10$; $q_4=Q_3^3=(Q_2q_3+Q_2)^3=75\,35\,71$, например $q_4=75\,35\,72$ и т. д. Таким образом, получаем $\alpha=(0, 1, 2, 10, 75\,35\,72, \ldots)$.

420. Рассмотрим рациональное число $r=\dfrac{1}{10^{1!}}+\dfrac{1}{10^{2!}}+\ldots+\dfrac{1}{10^{k!}}=\dfrac{c}{10^{k!}}$. Имеем $\alpha-r=\dfrac{1}{10^{(k+1)!}}+\dfrac{1}{10^{(k+2)!}}+\ldots<\dfrac{2}{10^{(k+1)!}}$, следовательно, $\alpha-r\to 0$ при $k\to\infty$. Таким образом, при $\dfrac{2}{10^{(k+1)!}}<\dfrac{\varepsilon}{(10^{k!})^n}$ имеет место $\alpha-r<\dfrac{\varepsilon}{(10^{k!})^n}$.

421. Данные числа иррациональны и им соответствуют алгебраические числа: 1) $10^{\lg 2}=2$; 2) $2^{\log_2 10}=10$; 3) $e^{\ln 5}=5$; 4) $x=\dfrac{\lg a}{\lg e}=\ln a$ или $a=e^x$, но в полученном равенстве при алгебраическом a число x должно быть трансцендентным.

422. 1) -3. 2) 11. 3) 1. 4) $\dfrac{10}{3+\sqrt{3}}=\dfrac{10(3-\sqrt{3})}{6}=\dfrac{1+2{,}6\ldots}{6}=2,\ldots$, откуда $\left[\dfrac{10}{3+\sqrt{3}}\right]=2$. 5) 3. 6) $3-1=2$. 7) $2-0=2$ (по формуле $[a-x]=a+[-x]$, где a — число целое и x — дробное). 8) $2-\lg 2512=2-3,\ldots=-1,\ldots$, откуда $[2-\lg 2512]=-2$. 9) -2, если $\overline{abcd}>1000$, и -1, если $\overline{abcd}=1000$. 10) $\sqrt[3]{30}+\sqrt[3]{10}=5{,}47\ldots+2{,}1\ldots=7,\ldots$, откуда $[\sqrt[3]{30}+\sqrt[3]{10}]=7$.

424. $\left[\dfrac{p}{4}\right]_{p=4n+1}=n=\dfrac{p-1}{4}$ и $\left[\dfrac{p}{4}\right]_{p=4n+3}=n=\dfrac{p-3}{4}$.

425. Имеем: $a=mq+1$, $0\leqslant r<m$, или $\frac{a}{m}=q+\frac{r}{m}, 0\leqslant\frac{r}{m}<1$, откуда $q=\left[\frac{a}{m}\right]$ и $\left[\frac{a}{m}\right]=\frac{a-r}{m}$.

426. Требуется доказать, что $\left[\frac{p+1}{4}\right]$ и $\frac{p^2-1}{8}$ — числа одинаковой четности. Рассмотреть случаи $p=4n+1$ и $p=4n+3$.

427. Данное соотношение равносильно соотношению $[nx]\leqslant nx<[nx]+1$, справедливость которого вытекает непосредственно из определения целой части числа nx.

428. $\frac{x+y}{n}=\left[\frac{x}{n}\right]+\alpha+\left[\frac{y}{n}\right]+\beta$, где $0\leqslant\alpha<1$ и $0\leqslant\beta<1$, откуда $\left[\frac{x+y}{n}\right]=\left[\frac{x}{n}\right]+\left[\frac{y}{n}\right]+[\alpha+\beta]$. Так как $0\leqslant\alpha+\beta<2$, то $[\alpha+\beta]$ равно либо 0, либо 1.

429. $m=10Q+r$, $0\leqslant r<10$, откуда $\frac{m}{10}=Q+\frac{r}{10}$, $0\leqslant\frac{r}{10}<1$ и $Q=\left[\frac{m}{10}\right]$.

430. Первый способ. $\left[\frac{m}{2}\right]_{m=2k+1}=\left[k+\frac{1}{2}\right]=k=\frac{m-1}{2}$.

Второй способ. Исследуемое соотношение равносильно следующему: $\frac{m-1}{2}\leqslant\frac{m}{2}<\frac{m+1}{2}$ или $-1\leqslant 0<1$. Но справедливость последнего очевидна.

431. См. рисунок 2, *а*, *б*, *в*.

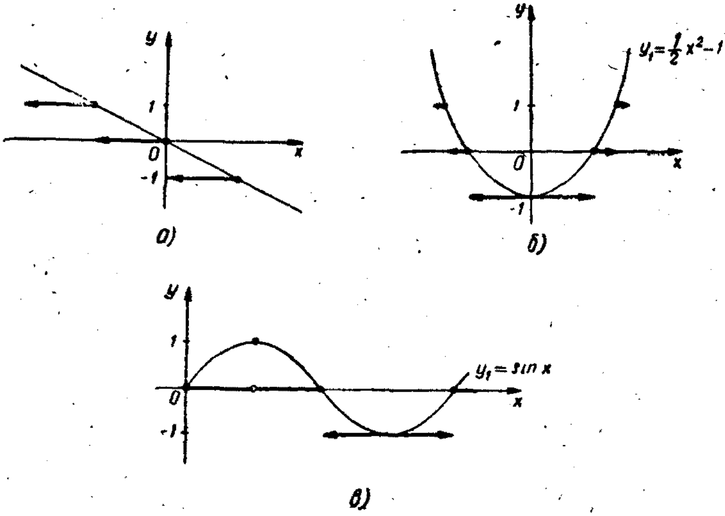

Рис. 2, *а*, *б*, *в*

432. 1) Имеем $2\leqslant x^2<3$ или $\sqrt{2}\leqslant|x|<\sqrt{3}$, откуда $-\sqrt{3}<x\leqslant-\sqrt{2}$ и $\sqrt{2}\leqslant x<\sqrt{3}$. 2) Необходимо, чтобы значения $x+1$, а следовательно, и x, были целочисленными. Но при этом значение $3x^2-x$ является целочисленным, и данное уравнение равносильно алгебраическому уравнению $3x^2-x=x+1$, откуда $x=1$. 3) Данному уравнению удовлетворяют $0\leqslant x<4$, при которых $\frac{3}{4}x$ принимает целочисленные значения, т. е. $x=0$; $1\frac{1}{3}$; $2\frac{2}{3}$. 4) $x=0$; 1.

Примечание. Данные уравнения полезно решить графически.

433. Данное условие может быть записано в виде $7\frac{1}{62}\leqslant m<7\frac{3}{31}$.

434. Если x — число целое, то $[-x]=-[x]$. При дробном значении x из $[-x]=y$ следует $-y-1<x<-y$ или $[x]=-y-1$ и $[-x]=-[x]-1$.

435. Если $[\log_a x]=-2$ или $-2\leqslant\log_a x<-1$, то $a^{-2}\leqslant x<a^{-1}$ при $a>1$ и $a^{-1}<x\leqslant a^{-2}$ при $0<a<1$.

436. $\sum\limits_{i=1}^{n}x_i=\sum\limits_{i=1}^{n}[x_i]+\sum\limits_{i=1}^{n}\alpha_i$, где $0\leqslant\alpha_i<1$, откуда $[\sum x_i]=$ $=\sum[x_i]+[\sum\alpha_i]$, где $[\sum\alpha_i]\geqslant0$.

437. Применить теорему задачи 436.

438. $\left[\frac{10^7}{786}\right]-\left[\frac{10^6}{786}\right]=11450.$

439. $999-\left[\frac{999}{5}\right]-\left[\frac{999}{7}\right]+\left[\frac{\left[\frac{999}{5}\right]}{7}\right]=686.$

440. $100-\left[\frac{100}{2}\right]-\left[\frac{100}{3}\right]+\left[\frac{100}{6}\right]=33.$

441. 488. Задача сводится к нахождению показателя степени, с которым 5 входит в каноническое разложение 1964!.

442. $\left[\frac{p^n}{p}\right]+\left[\frac{p^n}{p^2}\right]+\ldots+\left[\frac{p^n}{p^{n-1}}\right]+\left[\frac{p^n}{p^n}\right]=p^{n-1}+\ldots+p+$ $+1=\frac{p^n-1}{p-1}$. Например, $2^n!=2^{2^n-1}\cdot Q$, где $(Q, 2)=1$.

443. 48. Задача сводится к нахождению показателя степени, с которым 3 входит в каноническое разложение 100!.

444. $11!=2^8\cdot3^4\cdot5\cdot7\cdot11$.

445. $2^2\cdot11\cdot13\cdot17\cdot19$.

446. $N=\frac{1000!}{100!\,7^\alpha}$. Искомое значение α должно удовлетворять условию $\left[\frac{1000}{7}\right]+\left[\frac{1000}{49}\right]+\left[\frac{1000}{301}\right]=\left[\frac{100}{7}\right]+\left[\frac{100}{49}\right]+\alpha$, откуда $\alpha=148$.

447. 1) $(2m)!!=m!\cdot 2^m$, поэтому при $p=2$ искомый показатель равен $m+\sum\limits_{l=1}^{k}\left[\frac{m}{2^l}\right]$, где $2^k\leqslant m<2^{k+1}$; если же $p>2$, то имеем $\sum\limits_{l=1}^{s}\left[\frac{m}{p^l}\right]$, где $p^s\leqslant m<p^{s+1}$. 2) $(2m+1)!!=\frac{(2m+1)!}{(2m)!!}=\frac{(2m+1)!}{m!\,2^m}$. При $p>2$ имеем $\sum\limits_{l=1}^{k}\left[\frac{2m+1}{p^l}\right]-\sum\limits_{l=1}^{k}\left[\frac{m}{p^l}\right]$, где $p^k\leqslant 2m+1<p^{k+1}$.

448. а) Пусть $N=\overline{a_n\ldots a_1,\,a_0}_g$. Тогда $N\geqslant g^n$, откуда $\log_g N\geqslant n$. С другой стороны, $N\leqslant\overline{(g-1)(g-1)\ldots(g-1)}_g=g^{n+1}-1<g^{n+1}$, откуда $\log_g N<n+1$. Таким образом, $n\leqslant\log_g N<n+1$ и $n+1=[\log_g N]+1$. б) $[\log_2 4]=4$, откуда $16\leqslant N<32$. в) $[100\lg 12]+1=108$.

449. $Q_n(x)$ — число чисел вида m^n, $m=1, 2, 3, \ldots$, удовлетворяющих условию $1\leqslant m^n\leqslant x$, откуда $1\leqslant m\leqslant\sqrt[n]{x}$ и $Q_n(x)=\left[\sqrt[n]{x}\right]$.

Примечание. Условие, которому должно удовлетворять искомое число m, можно записать в виде $m^n\leqslant x<(m+1)^n$, откуда $m\leqslant\sqrt[n]{x}<m+1$ и $m=\left[\sqrt[n]{x}\right]$ или $Q_n(x)=\left[\sqrt[n]{x}\right]$. Например, $Q_3(180{,}5)=\left[\sqrt[3]{180{,}5}\right]=5$.

450. Искомое НОК есть некоторая функция $\psi(m)$. В каноническое разложение $\psi(m)$ входят все простые числа, не превышающие m: $p_1<p_2<\ldots<p_k\leqslant m$. При этом должно выполняться условие $p_i^x\leqslant m<p_i^{x+1}$, откуда

$$x=\left[\frac{\lg m}{\lg p_i}\right] \text{ и } \psi(x)=\prod_{i=1}^{k}p_i^{\left[\frac{\lg m}{\lg p_i}\right]}.$$

451. Любой целочисленной абсциссе $x=k$ $(a\leqslant k\leqslant b)$ соответствует $[f(x)]+1$ целочисленных ординат, заключенных внутри и на границе трапеции. Следовательно, искомое число точек равно $\sum\limits_{k=a}^{b}([f(k)]+1)$.

452. Беря первый координатный угол и применяя формулу предыдущей задачи, находим: $7+7+7+6+6+3+3=39$ точек. Но здесь каждый раз считаются точки, лежащие на вертикальных и горизонтальных радиусах, поэтому искомое число равно $39.4-7.4=126$.

453. По условию либо $a=4q+1$, либо $a=4q+3$. В первом случае $\left[\frac{a}{4}\right]+\left[\frac{2a}{4}\right]+\left[\frac{3a}{4}\right]=q+2q+3q=6q=\frac{3(a-1)}{2}$. Аналогично проверяется и второй случай.

454. Пусть $a=mq+r$, где $0\leqslant r<m$ и $(r, m)=1$. Так как условие $(r, m)=1$ должно иметь место при любом $m\leqslant 2$, то относительно r имеется единственная возможность: $r=1$. Таким образом, $\sum\limits_{i=1}^{m-1}\left[i\left(q+\frac{1}{m}\right)\right]=q\sum\limits_{i=1}^{m-1}=\frac{a-1}{m}\cdot\frac{m(m-1)}{2}$.

455. $x=[x]+\alpha$, где $0<\alpha<1$, откуда $[x]+\left[x+\frac{1}{2}\right]=2[x]+$ $+\left[\alpha+\frac{1}{2}\right]$, где $\frac{1}{2}\leqslant\alpha+\frac{1}{2}<1\frac{1}{2}$ и $\left[\alpha+\frac{1}{2}\right]$ либо 0, либо 1. Так как $2x=2[x]+2\alpha$ и $[2x]=2[x]+[2\alpha]$, то $[x]+$ $+\left[x+\frac{1}{2}\right]=[2x]-[2\alpha]+\left[\alpha+\frac{1}{2}\right]$. Остается проверить, что либо $\left[\alpha+\frac{1}{2}\right]=[2\alpha]=0$, либо $\left[\alpha+\frac{1}{2}\right]=[2\alpha]=1$.

456. Представив данное уравнение в виде $[x]=1+2\left[\frac{x}{2}\right]$ и обозначив левую часть через y, имеем:

$$\begin{cases} y=[x], \\ \frac{y-1}{2}=\left[\frac{x}{2}\right]. \end{cases}$$

Обозначая далее целое значение $\frac{y-1}{2}$ через m, получаем:

$$\begin{cases} 2m+1=[x], \\ m=\left[\frac{x}{2}\right] \end{cases} \quad \text{или} \quad \begin{cases} 2m+1\leqslant x<2m+2, \\ 2m\leqslant x<2m+2, \end{cases}$$

откуда $2m+1\leqslant x<2m+2$, $m=0;\ \pm1;\ \pm2;\ \ldots$. Полезно рассмотреть графическое решение данного уравнения.

457. Обозначив каждую часть уравнения через y, имеем $y<\frac{x}{m}<\frac{x}{m-1}<y+1$, откуда $my\leqslant x<(m-1)(y+1)$. Чтобы такие значения x существовали, необходимо и достаточно, чтобы $my<(m-1)(y+1)$ или $y<m-1$. Ответ: $my\leqslant x<(m-1)\times$ $\times(y+1)$, где y—целое число, удовлетворяющее условию $y<m-1$.

458. Функция ax^2+bx+c, а следовательно, и функция $[ax^2+$ $+bx+c]$ ограничены — снизу при $a>0$ и сверху при $a<0$. В обоих случаях точной границей значений функции $[ax^2+bx+c]$ служит число $\left[-\frac{b^2-4ac}{4a}\right]$. Поэтому при $a>0$ данное уравнение имеет решение тогда и только тогда, когда $\left[-\frac{b^2-4ac}{4a}\right]\leqslant d$; если же $a<0$, то условием существования решения является: $\left[-\frac{b^2-4ac}{4a}\right]\geqslant$ $\geqslant 1$.

459. При $p=3$ справедливость утверждения очевидна. Рассмотрим $p>3$. Слагаемые левой части данного равенства являются нулями и единицами, так как, например, при $p=4n+1$ имеем

$\left[\frac{4}{p}\right]=0$ и $\left[\frac{2(p-1)}{p}\right]=\left[\frac{8n}{4n+1}\right]=\left[\frac{4n+1+4n-1}{4n+1}\right]=\left[1+\frac{4n-1}{4n+1}\right]=1.$
Чтобы найти число слагаемых-нулей, достаточно в общем виде слагаемого $\left[\frac{2\cdot 2x}{p}\right]=\left[\frac{4x}{p}\right]$ положить $4x<p$ или $x<\frac{p}{4}$, откуда $x=\left[\frac{p}{4}\right]$. Значит, число слагаемых-единиц равно $\frac{p-1}{2}-\left[\frac{p}{4}\right]$, т. е. n, если $p=4n+1$, и $n+1$, если $p=4n+3$. Но и $\left[\frac{p+1}{4}\right]$ равно n, если $p=4n+1$, и $n+1$, если $p=4n+3$.

460. $\tau(600)=24$, $\sigma(600)=1860$.

461. Для нахождения делителей числа $m=\prod_{i=1}^{k}p_i^{\alpha_i}$ достаточно раскрыть скобки в выражении $\sigma(m)=(1+p_1+p_1^2+\ldots+p_1^{\alpha_1})\times$ $\times(1+p_2+p_2^2+\ldots+p_2^{\alpha_2})\ldots(1+p_k+p_k^2+\ldots+p_k^{\alpha_k})$.

462. См. рисунок 3.

463. $\sigma(p_1)=1+p_1=1+(p_2-2)=p_2-1=\varphi(p_2)$.

464. $\sigma(2^\alpha)=2^{\alpha+1}-1=2\times2^\alpha-1$, следовательно, $m=2^\alpha$, где α — любое натуральное число.

465. Воспользоваться формулами $\tau(m)=\prod_{i=1}^{k}(1+\alpha_i)$ и $\sigma(m)=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$, где $m=\prod_{i=1}^{k}p_i^{\alpha_i}$.

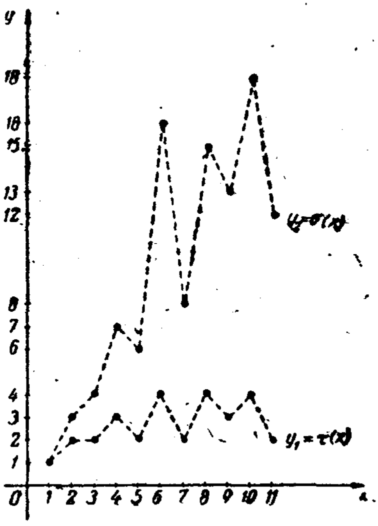

Рис. 3

466. Если p входит в каноническое разложение только m или только n с некоторым показателем α, то как $\tau(mn)$, так и $\tau(m)\cdot\tau(n)$ содержат множитель $\alpha+1$. Если же канонические разложения m и n содержат соответственно p^α и p^β, то каноническое разложение mn содержит $p^{\alpha+\beta}$, и множителю $\alpha+\beta+1$, содержащемуся в $\tau(mn)$, соответствует множитель $(\alpha+1)(\beta+1)>\alpha+\beta+1$, содержащийся в $\tau(m)\tau(n)$. Таким образом, если $(m, n)>1$ то $\tau(m)\tau(n)>\tau(mn)$. Относительно функции $\sigma(x)$ случай, когда p входит в каноническое разложение только m или только n, рассматривается аналогично.

Во втором случае множителю $\frac{p^{\alpha+\beta+1}}{p-1}$, входящему в $\sigma(mn)$, соответствует произведение $\frac{p^{\alpha+1}-1}{p-1}\cdot\frac{p^{\beta+1}-1}{p-1}=\frac{p^{\alpha+\beta+2}-p^{\alpha+1}}{(p-1)^2}+$ $+\frac{-p^{\beta+1}+1}{(p-1)^2}$, входящее в $\sigma(m)\sigma(n)$. Легко доказать, что

$$\frac{p^{\alpha+\beta+2}-p^{\alpha+1}-p^{\beta+1}+1}{p-1}-(p^{\alpha+\beta+1}-1)=\frac{p(p^{\alpha}-1)(p^{\beta}-1)}{p-1},$$

откуда $\frac{p^{\alpha+1}-1}{p-1}\cdot\frac{p^{\beta+1}-1}{p-1}>\frac{p^{\alpha+\beta+1}-1}{p-1}$. Таким образом, если $(m, n)>1$, то $\sigma(m)\sigma(n)>\sigma(mn)$.

467. Если $m=\prod_{i=1}^{k}p_i^{\alpha_i}$, то $\tau(m^n)=\prod_{i=1}^{k}(n\alpha_i+1)$, где $(n\alpha_i+1,n)=1$.

468. а) Пусть $d_1, d_2, \ldots, d_{\tau(m)}$ — все натуральные делители m. Тогда $\delta(m)=\prod_{i=1}^{\tau(m)}d_i$. Так как $\frac{m}{d_1}, \frac{m}{d_2}, \ldots, \frac{m}{d_{\tau(m)}}$ — те же делители m, то $\delta(m)=\prod_{i=1}^{\tau(m)}\frac{m}{d_i}=m^{\tau(m)}\prod_{i=1}^{\tau(m)}\frac{1}{d_i}$. Таким образом, $\delta^2(m)=$ $=m^{\tau(m)}$, откуда $\delta(m)=\sqrt{m^{\tau(m)}}$. б) $\delta(10)=\sqrt{10^4}=100$.

469. $m=2^4\cdot3\cdot41$; $\varphi(m)=640$; $\tau(m)=20$; $\sigma(m)=5208$; $\delta(m)=1968^{10}$.

470. Числа m, равные произведению всех своих натуральных делителей, определяются уравнением $m=\sqrt{m^{\tau(m)}}$, т. е. $\tau(m)=2$, откуда и следует справедливость теоремы.

471. Имеем $\sqrt{m^{\tau(m)}}=2^3\cdot3^6$, откуда $m=2^x\cdot3^y$ и

$$\begin{cases} x(1+x)(1+y)=6,\\ y(1+x)(1+y)=12.\end{cases}$$

Таким образом, $x=1, y=2$ и $m=18$.

472. $s_n(p^{\alpha})=1^n+p^n+(p^2)^n+\ldots+(p^{\alpha})^n=\frac{p^{n(\alpha+1)}-1}{p^n-1}$;

$$\begin{aligned} s_n(p_1^{\alpha_1}p_2^{\alpha_2})&=s_n(p_1^{\alpha_1})+\left[p_2^n+(p_1p_2)^n+(p_1^2p_2)^n+\ldots+(p_1^{\alpha_1}p_2)^n\right]+\\ &+\left[(p_2^2)^n+(p_1p_2^2)^n+(p_1^2p_2^2)^n+\ldots+(p_1^{\alpha_1}p_2^2)^n\right]+\ldots+\\ &+\left[(p_2^{\alpha_2})^n+(p_1p_2^{\alpha_2})^n+(p_1^2p_2^{\alpha_2})^n+\ldots+(p_1^{\alpha_1}p_2^{\alpha_2})^n\right]=\\ &=s_n(p_1^{\alpha_1})+p_2^n\cdot s_n(p_1^{\alpha_1})+p_2^{2n}s_n(p_1^{\alpha_1})+\ldots+p_2^{\alpha_2\cdot n}\cdot s_n(p_1^{\alpha_1})=\\ &=s_n(p_1^{\alpha_1})\cdot s_n(p_2^{\alpha_2})=\frac{p_1^{n(\alpha_1+1)}-1}{p_1^n-1}\cdot\frac{p_2^{n(\alpha_2+1)}-1}{p^n-1}.\end{aligned}$$

Теперь легко проследить „шаг" математической индукции: если $s_n\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)=\prod_{i=1}^{k}\frac{p_i^{n(\alpha_i+1)}-1}{p_i^n-1}$, то $s_n\left(\prod_{i=1}^{k+1} p_i^{\alpha_i}\right)=\prod_{i=1}^{k+1}\frac{p_i^{n(\alpha_i+1)}-1}{p_i^n-1}$.

Таким образом, если $m=\prod_{i=1}^{k} p_i^{\alpha_i}$, где k — любое натуральное число, то

$$s_n(m)=\prod_{i=1}^{k}\frac{p_i^{n(\alpha_i+1)}-1}{p_i^n-1}.$$

473. $\sigma(8128)=16256=2.8128.$

474. $\sigma(p^\alpha)=\frac{p^{\alpha+1}-1}{p-1}=p^\alpha+\ldots+p^2+p+1=p^\alpha+\frac{p^\alpha-1}{p-1}<$ $<2p^\alpha$.

475. $\sigma(m)=\sigma(p_1^{\alpha_1}p_2^{\alpha_2})=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}<\frac{p_1^{\alpha_1+1}}{p_1-1}\times$ $\times\frac{p_2^{\alpha_2+1}}{p_2-1}=m\cdot\frac{p_1}{p_1-1}\cdot\frac{p_2}{p_2-1}$. По условию $p_1\geqslant 3$ и $p_2\geqslant 5$, откуда $\frac{p_1}{p_1-1}\cdot\frac{p_2}{p_2-1}\leqslant\frac{3}{2}\cdot\frac{5}{4}<2$ и $\sigma(m)<2m$.

476. Пусть $2^\alpha(2^{\alpha+1}-1)=m$ и $2^{\alpha+1}-1=p$, тогда

$$\sigma(m)=\sigma(2^\alpha\cdot p)=(2^{\alpha+1}-1)(p+1)=(2^{\alpha+1}-1)\cdot 2^{\alpha+1}=2m.$$

477. Остается доказать, что любое четное совершенное число есть число вида $2^\alpha(2^{\alpha+1}-1)$, где $2^{\alpha+1}-1$ — число простое (задача 476). Пусть $m=2^\alpha\cdot q$, где $(q,2)=1$ и $\sigma(m)=2m$, т. е. $(2^{\alpha+1}-1)\,\sigma(q)=2^{\alpha+1}\cdot q$, откуда $\sigma(q)=2^{\alpha+1}\cdot k$ и $q=(2^{\alpha+1}-1)\,k$, где k — натуральное число. Так как k и $(2^{\alpha+1}-1)\,k$ являются делителями q и их сумма равна $k\cdot 2^{\alpha+1}=\sigma(q)$, то q других натуральных делителей не имеет. Следовательно, $q=(2^{\alpha+1}-1)\,k$—число простое (имеющее в точности два делителя). Значит, $k=1$ и $(2^{\alpha+1}-1)$ — число простое, что требовалось доказать.

478. Уравнение $\sigma(m)=3m$ при $m=2^\alpha\cdot p_1p_2$ принимает вид:

$$(2^{\alpha+1}-1)(1+p_1)(1+p_2)=3\cdot 2^\alpha\cdot p_1p_2.$$

При $\alpha=0$ имеем $(1+p_1)(1+p_2)=3p_1p_2$ или $1+p_1+p_2=2p_1p_2$, откуда p_1 и p_2 должны быть четными, что невозможно (так как $1+p_1$ и $1+p_2$ четные). Значит, $\alpha\neq 0$. При $\alpha=1$ имеем $(1+p_1)\times$ $\times(1+p_2)=2p_1p_2$ или $1+p_1+p_2=p_1p_2$, т. е. $1+p_1=p_2(p_1-1)$; так как, $p_1-1=2n$, то $n+1=p_2\cdot n$, откуда $n=1$ и $p_2=2$, что невозможно.

Значит, $\alpha \neq 1$. При $\alpha=2$ имеем $7(1+p_1)(1+p_2)=12\,p_1p_2$ или $7+7\times(p_1+p_2)=5\,p_1p_2$, откуда $p_1=7$ (или $p_2=7$) и $p_2=2$ (или $p_1=2$), что невозможно. Значит, $\alpha \neq 2$. При $\alpha=3$ имеем $5(1+p_1)(1+p_2)=8p_1p_2$ или $5+5(p_1+p_2)=3\,p_1p_2$, откуда $p_1=5$ и $p_2=3$. Таким образом, наименьшее натуральное число, удовлетворяющее условиям задачи, есть $m=2^3\cdot3\cdot5=120$.

479. По условию $m=p_1^{\alpha_1}\,p_2^{\alpha_2}$. Так как при этом $(1+p_1)(1+p_2)=6$, то $\alpha_1=1$, $\alpha_2=2$ и $m=p_1p_2^2$. Кроме того, $\sigma(m)=28$, т. е. $(1+p_1)\times(p_2^2+p_2+1)=28$, откуда $1+p_1=4$ и $p_2^2+p_2+1=7$, т. е. $p_1=3$ и $p_2=2$. Таким образом, $m=3\cdot2^2=12$.

480. $\tau(m)=14=2\cdot7=(1+1)(6+1)$, откуда $m=p_1^{\alpha_1}\,p_2^{\alpha_2}$, точнее, $m=2^{\alpha_1}\cdot3^{\alpha_2}$, где $\alpha_1\geqslant 2$ и $d_2\geqslant 1$. Значит, $m=2^6\cdot3=192$.

481. По условию $m=p_1^{\alpha_1}\,p_2^{\alpha_2}$, $m^2=p_1^{2\alpha_1}\cdot p_2^{2\alpha_2}$ и $(2\alpha_1+1)(2\alpha_2+1)=15$, откуда $2\alpha_1+1=3$ и $2\alpha_2+1=5$, т. е. $\alpha_1=1$ и $\alpha_2=2$. Значит, $\tau(m^3)=(3\alpha_1+1)(3\alpha_2+1)=4\cdot7=28$.

482. По условию $(1+2\alpha_1)(1+2\alpha_2)=81$, поэтому имеем две возможности: $(1+2\alpha_1)(1+2\alpha_2)=3\cdot27$ и $(1+2\alpha_1)(1+2\alpha_2)=9\cdot9$, т. е. $\alpha_1=1$, $\alpha_2=13$ и $\alpha_1=\alpha_2=4$, откуда либо $\tau(m^3)=160$, либо $\tau(m^3)=169$.

483. Так как $\tau\left(\frac{m}{2}\right)=x(y+1)(z+1)$, $\tau\left(\frac{m}{3}\right)=(x+1)\,y\,(z+1)$ и $\tau\left(\frac{m}{5}\right)=(x+1)(y+1)\,z$, то по условию $x(y+1)(z+1)+30=(x+1)\,y\,(z+1)+35=(x+1)(y+1)\,z+42=(x+1)(y+1)(z+1)$, откуда

$$\begin{cases}(y+1)(z+1)=30,\\(x+1)(z+1)=35,\\(x+1)(y+1)=42\end{cases}$$

и $x=6$, $y=5$, $z=4$.

484. Пусть $m=\prod\limits_{i=1}^{k}p_i^{\alpha_i}$. Тогда $\tau(m)=\prod\limits_{i=1}^{k}(1+\alpha_i)$. Если $\tau(m)\equiv 1\pmod 2$, то $1+\alpha_i\equiv 1\pmod 2$, откуда $\alpha_i\equiv 0\pmod 2$, а это означает, что m — квадрат целого числа. Обратно, если m — квадрат целого числа, то $\alpha_i\equiv 0\pmod 2$, откуда $\tau(m)\equiv 1\pmod 2$.

485. См. рисунок 4.

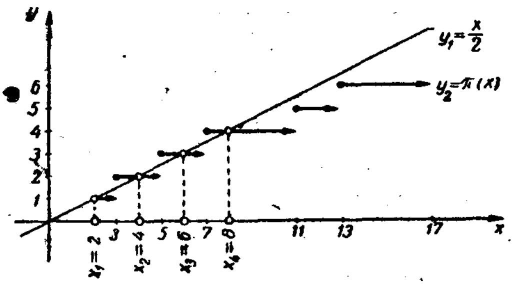

Рис. 4

486. $\pi(1000) \approx \frac{1000}{3 \cdot \ln 10} \approx \frac{1000}{6{,}9078} \approx 145$. По таблице же простых чисел $\pi(1000) = 168$. Следовательно, $\frac{\Delta\pi(1000)}{\pi(1000)} = \frac{168-145}{168} \approx 14\%$.

487. Из $a < \pi(x) : \frac{x}{\ln x} < b$ следует $\frac{a}{\ln x} < \frac{\pi(x)}{x} < \frac{b}{\ln x}$. Так как, кроме того, $\lim\limits_{x\to+\infty} \frac{a}{\ln x} = \lim\limits_{x\to+\infty} \frac{b}{\ln x} = 0$, то $\lim\limits_{x\to+\infty} \frac{\pi(x)}{x} = 0$.

Замечание. Из доказанного следует, что функция $\pi(x)$ растет медленнее, чем x. Отношение $\frac{\pi(x)}{x}$ Эйлер рассматривал как среднюю плотность простых чисел на отрезке $[1, x]$.

488. Исходя из очевидного неравенства $\pi(p) < p$, получаем: $-p < -\pi(p)$, $p\pi(p) - p < (p-1)\pi(p)$ и $\frac{\pi(p)-1}{p-1} < \frac{\pi(p)}{p}$. Так как $\pi(p) - 1 = \pi(p-1)$, то имеем: $\frac{\pi(p-1)}{p-1} < \frac{\pi(p)}{p}$. Исходя из очевидного равенства $\pi(m-1) = \pi(m)$, получаем: $\frac{\pi(m)}{m} < \frac{\pi(m-1)}{m-1}$.

ТАБЛИЦА ИНДЕКСОВ ПО ПРОСТЫМ МОДУЛЯМ, МЕНЬШИМ 100.

Данная таблица размещена на трех страницах (стр. 121—123). На первых двух страницах (стр. 121 и 122) индексы даны для всех простых модулей от 3 до 97 (для чисел от 1 до 20 и от 21 до 40). На третьей странице (стр. 123) индексы даны в виде трех отдельных табличек соответственно для простых модулей от 43 до 97, от 67 до 97 и от 83 до 97 (и соответственно для чисел от 41 до 60, от 61 до 80 и от 81 до 96).

Таким образом, таблица подразделена (по соображениям экономии бумаги) на пять неравных по объему частей. В каждой из этих пяти частей числа выделены в виде колонок двумя вертикальными жирными линиями.

Внутри таблицы на пересечении строк и столбцов даны численные значения индексов, соответствующие числу, равному номеру строки, и по модулю, равному номеру столбца.

Приведем примеры нахождения индексов по данной таблице.

Пример 1. Дано число 28 и модуль 59. Найти соответствующий им индекс.

Решение. В таблице (стр. 121) находим 28-ю строку и 59-й столбец, на пересечении этих строки и столбца читаем индекс, равный 10.

Пример 2. Дано число 66 и модуль 67. Найти соответствующий им индекс.

Решение. В таблице (стр. 123) на пересечении 66-й строки и 67-го столбца читаем 33. Это и есть искомый индекс.

Пример 3. Дан индекс 80 и модуль 83. Найти число.

Решение. В столбце 83 находим индекс 80. Этот индекс стоит в строке 10. Это и будет искомое число.

Пример 4. Дано число 86 и индекс 45. Найти модуль.

Решение. Находим в таблице (стр. 123) строку 86 и на этой строке находим индекс 45. Этот индекс стоит в столбце 89. Искомый модуль будет 89.

Таблицы индексов по простым модулям, меньших 100

Числа	Модули 3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	Числа
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
2	1	3	4	3	7	14	7	12	17	24	11	14	27	18	49	15	31	17	6	8	4	79	16	34	2
3		1	5	4	4	1	1	8	1	1	34	25	1	20	1	54	6	3	26	6	1	30	1	70	3
4		2	2	6	2	12	14	2	6	18	22	28	12	36	46	30	2	34	12	16	8	76	32	68	4
5			1	2	3	5	4	17	10	20	1	18	25	1	15	32	22	57	28	1	62	1	70	1	5
6			3	7	11	15	8	20	18	25	9	39	28	38	50	11	37	20	32	14	5	27	17	8	6
7				1	5	11	6	15	8	28	28	1	35	32	10	38	19	61	1	33	53	58	81	31	7
8				9	9	10	3	14	23	12	33	2	39	8	43	45	33	51	18	24	12	73	48	6	8
9				8	8	2	2	16	2	2	32	10	2	40	2	50	12	6	52	12	2	60	2	44	9
10				5	10	3	11	7	27	14	12	32	10	19	12	47	53	8	34	9	66	80	86	35	10
11					1	7	12	21	5	23	6	37	30	7	34	27	45	13	31	55	68	10	84	6	11
12					6	13	15	10	7	19	20	13	13	10	47	26	8	37	38	22	9	24	33	42	12
13						4	17	18	26	11	13	9	32	11	32	37	40	59	39	59	34	15	23	25	13
14						9	13	5	25	22	3	15	20	4	7	53	50	12	7	41	57	55	9	65	14
15						6	5	3	11	21	35	3	26	21	16	28	28	60	54	7	63	31	71	71	15
16						8	10	4	12	6	8	16	24	26	40	2	4	2	24	32	16	70	64	40	16
17							16	9	21	7	5	7	38	16	22	20	17	32	49	21	21	78	6	89	17
18							9	6	19	26	7	24	29	12	51	7	43	23	58	20	6	57	18	78	18
19								13	13	4	25	31	19	45	45	48	26	38	16	62	32	23	35	81	19
20								19	16	8	23	6	37	37	9	4	24	25	40	17	70	77	14	69	20

Продолжение

Числа	Модули																								Числа
	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	
21								1	9	29	26	26	36	6	11	34	25	64	27	39	54	6	82	5	21
22								11	22	17	17	11	16	25	31	42	16	30	37	63	72	7	12	24	22
23									4	27	21	4	16	5	39	51	27	14	15	46	26	66	57	77	23
24									24	13	31	27	40	28	44	41	39	54	44	30	13	21	49	76	24
25									20	10	2	36	8	2	30	6	44	48	56	2	46	2	52	2	25
26									15	5	24	23	17	29	29	52	11	10	45	67	38	12	39	59	26
27									3	3	30	35	3	14	3	46	18	9	8	18	3	8	3	18	27
28									14	16	14	29	5	22	4	10	21	29	13	49	61	52	25	3	28
29										9	15	33	41	35	18	14	5	22	68	35	11	46	59	13	29
30										15	10	17	11	39	13	43	59	11	60	15	67	28	87	9	30
31											27	12	34	3	5	39	29	7	11	11	56	50	31	46	31
32											19	30	9	44	37	17	35	19	30	40	20	67	80	74	32
33											4	22	31	27	35	23	51	16	57	61	69	40	85	60	33
34											16	21	23	34	19	35	48	49	55	29	25	75	22	27	34
35											29	19	18	33	25	12	41	52	29	34	37	59	63	32	35
36											18	38	14	30	48	22	14	40	64	28	10	54	34	16	36
37												8	7	42	14	13	9	44	20	64	19	22	11	91	37
38												5	4	17	42	5	57	55	22	70	36	20	51	19	38
39												34	33	31	33	33	46	62	65	65	35	45	24	95	39
40												20	22	9	6	19	55	42	46	25	74	74	30	7	40

Продолжение

Числа	Модули											
	43	47	53	59	61	67	71	73	79	84	89	97
41	6	15	21	36	54	43	25	4	75	44	21	85
42	21	24	8	49	56	15	33	47	58	3	10	39
43		13	38	31	13	21	48	51	49	33	29	4
44		43	28	57	47	47	43	71	76	4	28	58
45		41	17	24	34	63	10	13	64	61	72	45
46		23	36	8	58	31	21	54	30	63	73	15
47			24	55	20	58	9	31	59	13	54	84
48			41	56	10	5	50	38	17	18	65	14
49			20	18	38	56	2	66	28	34	74	62
50			27	21	15	65	62	10	50	81	68	36
51			23	16	23	35	5	27	22	26	7	63
52			26	9	42	27	51	3	42	9	55	93
53				40	3	45	23	53	77	69	78	10
54				3	49	26	14	26	7	5	19	52
55				1	7	4	59	56	52	11	66	87
56				25	52	46	19	57	65	49	41	37
57				44	32	41	42	68	33	53	36	55
58				29	36	39	4	43	15	43	75	47
59					1	18	3	5	31	62	43	67
60					30	28	66	23	71	25	15	43

Продолжение

Числа	Модули						
	67	71	73	79	88	89	97
61	53	69	58	45	48	69	64
62	24	17	19	60	47	47	80
63	1	53	45	55	36	83	75
64	36	36	48	24	64	8	12
65	50	67	60	18	16	5	26
66	33	63	69	73	37	13	94
67		47	50	48	29	56	57
68		61	37	29	72	38	61
69		41	52	27	14	58	51
70		35	42	41	56	79	66
71			44	51	65	62	11
72			36	14	51	50	50
73				44	39	20	28
74				23	19	27	29
75				47	32	53	72
76				40	17	67	53
77				43	68	77	21
78				39	42	40	33

Окончание

Числа	Модули		
	83	89	97
79	35	42	30
80	71	46	41
81	38	4	88
82	41	37	23
83		61	17
84		26	73
85		76	90
86		45	38
87		60	83
88		44	92
89			54
90			79
91			56
92			49
93			20
94			22
95			82
96			48

ТАБЛИЦА ПРОСТЫХ ЧИСЕЛ, МЕНЬШИХ 1000

2	47	109	191	269	353	439	523	617	709	811	907
3	53	113	193	271	359	443	541	619	719	821	911
5	59	127	197	277	367	449	547	631	727	823	919
7	61	131	199	281	373	457	557	641	733	827	929
11	67	137	211	283	379	461	563	643	739	829	937
13	71	139	223	293	383	463	569	647	743	839	941
17	73	149	227	307	389	467	571	653	751	853	947
19	79	151	229	311	397	479	577	659	757	857	953
23	83	157	233	313	401	487	587	661	761	859	967
29	89	163	239	317	409	491	593	673	769	863	971
31	97	167	241	331	419	499	599	677	773	877	977
37	101	173	251	337	421	503	601	683	787	881	983
41	103	179	257	347	431	509	607	691	797	883	991
43	107	181	263	349	433	521	613	701	809	887	997

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

Виноградов И. М., Основы теории чисел, Гостехиздат, Москва, 1953.

Бухштаб А. А., Теория чисел, Учпедгиз, Москва, 1960

Арнольд И. В., Теория чисел, Учпедгиз, Москва, 1939.

Лежен-Дирихле П. Г., Лекции по теории чисел, Гостехиздат, Москва — Ленинград, 1936.

Хассе Г., Лекции по теории чисел, Издательство иностранной литературы, Москва, 1953.

Сушкевич А. К., Теория чисел (элементарный курс), Издательство Харьковского университета, 1954.

Окунев Л. Я., Краткий курс теории чисел, Учпедгиз, Москва, 1956.

Михелович Ш. Х., Теория чисел, «Высшая школа», Москва, 1967.

Хинчин А. Я., Элементы теории чисел, Гостехиздат, Москва — Ленинград, 1951.

Его же, Цепные дроби, Гостехиздат, Москва — Ленинград, 1949.

Гребенча М. К., Теория чисел, Учпедгиз, Москва, 1949.

Глаголев Н. А., Курс теоретической арифметики и сборник теоретических упражнений, Москва, 1914.

Таннери Ж., Курс теоретической и практической арифметики, Москва, 1913.

Александров В. А. и Горшенин С. М., Задачник-практикум по теории чисел, Учпедгиз, Москва, 1963.

Архангельская В. М., Элементарная теория чисел, Издательство Саратовского университета, 1962.

Грибанов В. У. и Титов П. И., Сборник упражнений по теории чисел, «Просвещение», Москва, 1964.

Радемахер Г. и Теплиц О., Числа и фигуры, ОНТИ, Москва — Ленинград, 1935.

Берман Г. Н., Число и наука о нем, Физматгиз, Москва, 1960.

Воробьев Н. Н., Признаки делимости, Физматгиз, Москва, 1963.

Шклярский Д. О. и др., Избранные задачи и теоремы элементарной математики, часть I, Гостехиздат, Москва, 1954.

Кречмар В. А., Задачник по алгебре, Гостехиздат, Москва — Ленинград, 1950.

Серпинский В., Что мы знаем и чего мы не знаем о простых числах, Физматгиз, Москва — Ленинград, 1963.

Трост Э., Простые числа, Физматгиз, Москва, 1959.

Дэвенпорт Г., Высшая арифметика, «Наука», Москва, 1965.

Шнилерман Л. Г., Простые числа, Гостехиздат, Москва — Ленинград, 1940.

Диксон Л. Е., Введение в теорию чисел, Изд. АН Груз. ССР, Тбилиси, 1941.

Нивен А., Числа рациональные и иррациональные, «Мир», Москва, 1966.

ОГЛАВЛЕНИЕ

Гелий Александрович Кудреватов

СБОРНИК ЗАДАЧ ПО ТЕОРИИ ЧИСЕЛ

Редакторы *В. Г. Долгополов*
и *М. В. Яковкин*
Переплет *Е. М. Батыря*
Художественный редактор *В. С. Эрденко*
Технический редактор *Е. К. Полукарова*
Корректор *Р. Ю. Грошева*

Сдано в набор 12/IX 1969 г. Подписано к печати 12/VIII—1970 г. $84\times108^{1}/_{32}$. Бум. типографская № 2 Печ. л. 4,0 Усл. п. 6,72 Уч.-изд. л. 5,9 Тираж 40 000 экз. (Тем. пл. 1970 г. № 19) А03782

Издательство «Просвещение» Комитета по печати при Совете Министров РСФСР. Москва, 3-й проезд Марьиной рощи, 41.

Типография № 2 Росглавполиграфпрома, г. Рыбинск, ул. Чкалова, 8. Заказ 2956

Цена 17 коп.