. ГРИБАНОВ, П. И. ТИТОВ

СБОРНИК УПРАЖНЕНИЙ ПО ТЕОРИИ ЧИСЕЛ

ТЕЛЬСТВО «ПРОСВЕЩЕНИЕ»
Москва 1964

Книга рекомендована ученой комиссией по математике ГУВУЗ'а Министерства просвещения РСФСР в качестве учебного пособия для педагогических институтов.

ПРЕДИСЛОВИЕ

Предлагаемый сборник упражнений предназначается для проработки курса теории чисел в педагогических институтах.

Упражнения довольно резко разделяются на два типа. С одной стороны, дано большое количество упражнений тренировочного характера, предназначенных для выработки студентами вычислительных навыков и иллюстрирующих основные положения курса. Количество таких упражнений, по мнению авторов, вполне достаточно для аудиторных занятий, для самостоятельной работы студентов и для контрольных работ. Каждый номер этого типа содержит ряд примеров. Для некоторых примеров, обычно первых, даны решения, что особенно необходимо для студентов заочных отделений; некоторые примеры снабжены ответами; часть примеров, отмеченных звездочкой (*), оставлена без решений и ответов и предназначается для контрольных работ.

С другой стороны, дано значительное количество упражнений на доказательство и обоснование тех или иных предложений теоретического и числового характера, расширяющих кругозор будущего учителя математики в области учения о числе. Почти для всех упражнений этого типа даны решения, так как самостоятельное выполнение их студентами составляет значительные трудности. Условия большинства этих упражнений и некоторые решения заимствованы из курсов по теории чисел и других источников.

Каждому параграфу предпосланы краткие сведения из теории, необходимые для решения упражнений.

Сборник будет полезен и учителям математики средней школы в смысле использования многих упражнений с их решениями на занятиях в математических кружках.

Авторы сознают, что сборник не лишен недостатков, так как представляет собой первое приближение к сборнику упражнений по теории чисел.

Все замечания читателей о недостатках сборника будут приняты с большой благодарностью.

Выражаем глубокую признательность В. И. Нечаеву и П. Н. Реморева, внимательно прочитавшим рукопись и сделавшим ряд ценных замечаний.

Авторы

ГЛАВА I

ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ

§ 1. Основные понятия

Целыми числами называются числа ряда ..., —3, —2, —1, 0, 1, 2, 3, ..., т. е. не только натуральные числа 1, 2, 3, ... (положительные целые), но также нуль и отрицательные целые —1, —2, —3, ...

Как правило, при изложении материала мы будем обозначать буквами только целые числа. Случаи, когда буквы могут обозначать и нецелые числа, будем особо оговаривать.

Сумма, разность и произведение двух целых чисел a и b есть также целые, но частное от деления a на b (если b не равно нулю) может быть как целым, так и нецелым.

В случае, когда частное от деления числа a на число b является целым, обозначая его буквой q, имеем:

$$a = bq, \text{ или } \frac{a}{b} = q.$$

В этом случае говорят, что a *делится* на b, или b *делит* a. При этом a называют *кратным* числа b и b — *делителем* числа a. Утверждение, что b делит a, будем иногда кратко записывать так: b/a; если же b не делит a, то будем писать b/a.

В общем случае, включающем и частный, когда a делится на b, имеем следующую теорему: *всякое целое a представляется единственным образом через положительное целое b в форме* $a = bq + r$, *где* $0 \leqslant r < b$. Число q называется *неполным частным*, число r — *остатком* от деления a на b.

Приведем еще следующие две основные теоремы о делимости.

1. *Если a делится на b, b делится на c, то a делится на c*, т. е. если $a = cq_1$ и $b = cq_2$, то $a = cq$.

2. *Если каждое из чисел a и b делится на c, то сумма и разность их также делятся на c*, т. е. если $a = cq_1$ и $b = cq_2$, то $a + b = cq$ и $a - b = cq'$.

---

1. Число $a = 42\,157$ при делении на некоторое целое положительное число b дало в частном $q = 231$. Найти делитель b и остаток r.

2. Показать, что если $mn + pq$ делится на $m - p$, то и $mq + np$ делится на $m - p$, где m, n, p, q—целые числа.

3. Дано, что a, b, c, d, n — целые числа, удовлетворяющие условиям: $ad - bc$ делится на n, $a - b$ делится на n и числа b и n не имеют общих натуральных делителей, отличных от единицы. Показать, что $c - d$ делится на n.

4. Показать, что если пятизначное число делится на 41, то и все числа, получаемые путем круговой перестановки цифр этого числа, делятся на 41.

5. Показать, что $m^5 - m$, где m — натуральное число, делится на 30.

6. Некоторое шестизначное число оканчивается цифрой 5; если эту цифру переставить на первое место слева, то получится новое число, в 4 раза большее первоначального. Найти это число.

7. Показать, что $n(n + 1)(2n + 1)$, где n — натуральное число, делится на 6.

8. Показать, что $n(n^2 + 5)$, где n — натуральное число, делится на 6.

9. Показать, что если числитель дроби есть разность квадратов двух нечетных чисел, а знаменатель — сумма квадратов тех же чисел, то такая дробь всегда сократима на 2, но несократима на 4.

10. Найти четырехзначное число, являющееся точным квадратом, у которого цифра тысяч одинакова с цифрой десятков, а цифра сотен на 1 больше цифры единиц.

11. Показать, что сумма квадратов пяти последовательных целых чисел не может быть точным квадратом.

12. Если остаток от деления некоторого числа на 9 есть одно из чисел 2, 3, 5, 6, 8, то это число не может быть точным квадратом.

13. Найти сумму n членов ряда:

$$S_n = 7 + 77 + 777 + \ldots + \underbrace{77\ldots7}_{n \text{ цифр}}.$$

14. Показать, что при любом натуральном $n > 1$ числа вида $2^{2^n} + 1$ оканчиваются цифрой 7.

15. Показать, что числа 48, 4488, 444 888, ... могут быть представлены в виде произведения двух последовательных четных чисел.

16. Между цифрами числа 16 вписывают 15, в середину числа 1156 опять вписывают 15 и т. д. Показать, что все полученные числа будут точными квадратами.

17. Показать, что при любых натуральных m и n $mn(m^4 - n^4)$ делится на 30.

18. Доказать, что ни при каких целых x выражение $3x^2 + 2$ не является полным квадратом.

19. Пишут одну за другой четыре последовательные цифры, затем первые две переставляют одну на место другой, и таким образом получают четырехзначное число, представляющее точный квадрат. Найти это число.

20. Некоторое трехзначное число, написанное в семиричной системе, изображается теми же цифрами, но только в обратном порядке, если написать его в девятиричной системе счисления. Найти это число.

21. Показать, что при любом натуральном n произведение $(n + 1)(n + 2) \ldots (n + n)$ делится на 2^n.

§ 2. Наибольший общий делитель и наименьшее общее кратное

Всякое целое число, делящее одновременно целые числа $a, b, \ldots, l$, называется их *общим делителем*.

Самый большой из общих делителей называется *наибольшим общим делителем* (НОД) и обозначается $d = (a, b, \ldots, l)$.

Если $(a, b, \ldots, l) = 1$, то числа $a, b, \ldots, l$ называются *взаимно простыми*. Если каждое из чисел $a, b, \ldots, l$ взаимно просто с каждым другим из них, то числа $a, b, \ldots, l$ называются *попарно простыми*. Очевидно, что попарно простые числа всегда и взаимно просты; в случае же двух чисел понятия «попарно простые» и «взаимно простые» совпадают.

Для разыскания наибольшего общего делителя двух чисел применяется *алгорифм Евклида*, который состоит в следующем. Если a и b — натуральные числа и $a > b$, то

$$\begin{aligned}
a &= bq_1 + r_1, && \text{где } 0 < r_1 < b,\\
b &= r_1q_2 + r_2, && \text{где } 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, && \text{где } 0 < r_3 < r_2,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && \text{где } 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1}, && \text{где } r_{n+1} = 0.
\end{aligned}$$

Последний отличный от нуля остаток r_n и является наибольшим общим делителем чисел a и b.

При нахождении наибольшего общего делителя нескольких чисел $a, b, c, \ldots, l$ с помощью алгорифма Евклида сначала находится наибольший общий делитель d_1 чисел a и b, т. е. $d_1 = (a, b)$, затем $d_2 = (d_1, c)$ и т. д.

Способ нахождения НОД двух и нескольких чисел с помощью разложения их на простые множители считаем известным читателю из курса элементарной арифметики.

* * *

Всякое целое число, кратное всех данных чисел $a, b, \ldots, l$, называется их *общим кратным*. Наименьшее положительное общее кратное называется *наименьшим общим кратным* (НОК) и обозначается так:

$$m = [a, b, \ldots, l].$$

Общий вид всех общих кратных чисел a и b выражается равенством

$$M = \frac{ab}{d}t,$$

где t — целое число и $d = (a, b)$.

При $t = 1$ получаем наименьшее общее кратное чисел a и b:

$$m = \frac{ab}{d}, \text{ или } [a, b] = \frac{ab}{(a, b)}.$$

Наименьшее общее кратное попарно простых чисел равно их произведению.

Нахождение НОК двух и нескольких чисел с помощью разложения их на простые множители считаем известным читателю из курса элементарной арифметики.

---

22. Пользуясь алгорифмом Евклида, найти наибольший общий делитель следующих систем чисел:

1) 546 и 231; 2) 1001 и 6253; 3)* 1517 и 2257; 4) 2737, 9163 и 9639; 5)* 1411, 4641 и 5253.

23. Разложением на простые множители найти наименьшее общее кратное следующих систем чисел:

1) 360 и 504; 2) 2520 и 6600; 3) 187 и 533;

4)* 9163, 2737, 9639; 5)* 374, 1599 и 9061.

24. Доказать, что если $a = cq + r$ и $b = cq_1 + r_1$, где a, b, q, q_1, r, r_1 — целые неотрицательные числа и c — целое положительное число, то $(a, b, c) = (c, r, r_1)$. Сформулировать вытекающее отсюда правило нахождения (a, b, c). Обобщить правило на случай n чисел.

25. Пользуясь выведенным в предыдущей задаче правилом, найти наибольший общий делитель следующих систем чисел: 1) 299, 391 и 667; 2) 588, 2058 и 2849; 3) 31 605, 13 524, 12 915 и 11 067; 4)* 279, 372 и 1395; 5)* 2988, 3735, 8134 и 14 525.

26. По формуле $[a, b] = \frac{ab}{(a, b)}$ найти наименьшее общее кратное следующих пар чисел:

1) 252 и 468; 2) 279 и 372; 3) 178 и 381;

4)* 318 и 477; 5)* 758 и 1137.

Указание. НОД находить с помощью алгорифма Евклида. Проверить ответы путем отыскания НОК разложением чисел на простые множители.

27. Дано: $(a, b) = 24$, $[a, b] = 2496$. Найти a и b.

28. Сумма двух чисел 667, а отношение НОК к их НОД равно 120. Найти эти числа.

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

30. Дано: $a = 899$, $b = 493$. Найти $d = (a, b)$ и определить x и y, посредством которых можно осуществить линейное представление НОД в виде:

$$d = ax + by.$$

31. Решить предыдущую задачу для следующих пар чисел: 1) $a = 1445$, $b = 629$; 2) $a = 903$, $b = 731$; 3) $a = 1786$, $b = 705$; 4)* $a = 4543$, $b = 885$; 5)* $a = 6919$, $b = 1443$.

32. Доказать, что если a, b, c — нечетные числа, то

$$(a, b, c) = \left(\frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}\right).$$

33. Доказать, что

1) $[a, b, c] = \dfrac{abc\,(a, b, c)}{(a, b)\,(a, c)\,(b, c)}$;

2) $(a, b)\,(a, c)\,(b, c)\,[a, b]\,[a, c]\,[b, c] = a^2b^2c^2$.

34. Показать, что для любых натуральных a и b имеет место равенство:

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

35. Если $(a, b) = 1$, то $\dfrac{1}{a} + \dfrac{1}{a+b}$ —

несократимая дробь.

§ 3. Простые и составные числа

Натуральное число p, большее 1, называется *простым*, если оно имеет только два различных натуральных делителя (единицу и само p), и натуральное число a, большее 1, называется *составным*, если оно имеет больше двух различных натуральных делителей.

Число 1 имеет только один натуральный делитель — единицу, поэтому оно и не простое и не составное.

Наименьший натуральный делитель составного числа a, отличный от 1, есть число простое и не превосходит $\sqrt{a}$. Это позволяет при отыскании простых делителей числа a испытывать числа, не превосходящие $\sqrt{a}$.

Для составления таблицы простых чисел, не превосходящих данного a, существует общий способ, называемый *решетом Эратосфена*. Он сводится к установлению первого простого числа p_1 в данном натуральном ряду чисел и к вычеркиванию всех чисел, кратных p_1; затем к установлению второго простого числа p_2 и к вычеркиванию всех чисел, кратных p_2, и т. д., т. е. к вычеркиванию в натуральном ряду от 1 до a всех составных чисел, кратных простым, меньшим $\sqrt{a}$.

Всякое целое число a, большее единицы, можно представить в виде произведения простых множителей $p_1, p_2, \ldots, p_n$, и притом единственным способом (без учета порядка следования сомножителей):

$$a = p_1\ p_2\ \ldots\ p_n.$$

Некоторые сомножители могут повторяться, поэтому, обозначая буквами $\alpha_1, \alpha_2, \ldots, \alpha_n$ кратность их вхождения в a, получим *каноническое представление* числа a в виде произведения:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n};$$

любой делитель числа a будет иметь вид:

$$D = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},$$

где $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2, \ldots, 0 \leqslant \beta_n \leqslant \alpha_n$.

---

36. Исследовать, какие из чисел между 2320 и 2350 являются простыми.

37.* То же между числами 2640 и 2680.

38.* Найти все простые числа между числами 1300 и 1350.

39. Разложить на простые множители число $2^{18} + 3^{18}$.

40. Показать, что при натуральном $n > 1$ число $n^4 + 4$ составное. То же для $n^4 + n^2 + 1$.

41. Найти значения простого числа p, если известно, что $4p^2 + 1$ и $6p^2 + 1$ — тоже простые числа.

42. Найти значения простого числа p, если известно, что $p + 10$ и $p + 14$ — тоже простые числа.

43. Показать, что существует бесчисленное множество простых чисел вида $p = 6k - 1$.

44. Показать, что три числа a, $a + m$, $a + n$ не могут быть одновременно простыми, если $a > 3$ и натуральные числа m и n дают при делении на 3 остатки, соответственно равные 1 и 2.

45. Показать, что из всех целых чисел вида $2p + 1$, где p — простое число, только одно число является точным кубом.

46. Если перенумеровать все простые числа, начиная с 5, то каждое простое число будет больше своего утроенного номера.

47. Показать, что если простое число $p > 5$, то его квадрат при делении на 30 должен давать остаток, равный 1 или 19.

48. Показать, что если p и q — простые числа, большие 3, то $p^2 - q^2$ кратно 24.

49. Если нечетное число p может быть представлено в виде разности квадратов двух натуральных чисел единственным образом, то оно простое, в противном случае p — составное.

50. Пользуясь замечанием к решению предыдущей задачи, разложить на множители числа: 1) 6643; 2) 1769; 3) 3551; 4) 6497; 5)* 1817; 6)* 2407.

51. Доказать, что если число N может быть представлено в виде суммы квадратов двумя способами: $N = a^2 + b^2 = c^2 + d^2$, то оно составное.

52. Разложить на множители число $235^2 + 972^2$.

53. Разложить на множители число $3^{10} + 3^5 + 1$.

54. Если простое число имеет вид $1 + 2^k$, то $k = 0$ или $k = 2^n$ ($n = 0, 1, 2, \ldots$).

55. Число $a^\alpha + b^\beta$, где $(a, b)=1$, может быть простым тогда, когда $(\alpha, \beta) = 1$ или $(\alpha, \beta) = 2^k$.

56. Если $2^n - 1$ простое число, то и n — простое число.

ГЛАВА II

ЧИСЛОВЫЕ ФУНКЦИИ

§ 4. Функция $\pi(x)$

Функция $\pi(x)$ определяется для всех натуральных x и представляет собой количество простых чисел в натуральном ряду, не превосходящих x. Значение $\pi(x)$ находится точно непосредственным подсчетом простых чисел в натуральном ряду (обычно с использованием таблицы простых чисел) или, при больших значениях x, приближенно по формулам:

$$\pi(x) \approx \frac{x}{\ln x} \text{ и } \pi(x) \approx \int_2^x \frac{du}{\ln u}.$$

---

57. Найти точные значения: 1) $\pi(4)$; 2) $\pi(7)$; 3) $\pi(10)$; 4) $\pi(12)$; 5) $\pi(25)$; 6)* $\pi(37)$; 7) $\pi(50)$; 8)* $\pi(100)$; 9) $\pi(200)$; 10)* $\pi(300)$; 11) $\pi(500)$; 12)* $\pi(1000)$.

58. По формуле $\pi(x) \approx \frac{x}{\ln x}$ найти приближенные значения и относительные погрешности их:

1) $\pi(50)$; 2) $\pi(100)$; 3) $\pi(500)$; 4) $\pi(1000)$; 5) $\pi(5000)$; 6) $\pi(10\,000)$.

Указание. Натуральные логарифмы чисел в примерах 3)—6) можно найти как логарифмы произведений меньших чисел, например $\ln 500 = \ln 10 + \ln 50$.

§ 5. Функция $[x]$

Функция $[x]$ определяется для всех вещественных x и представляет собой наибольшее целое число, не превосходящее x. Эта функция называется *целой частью* x.

59. Найти: 1) $\left[\frac{8}{3}\right]$; 2) $\left[\frac{4}{5}\right]$; 3) $[2{,}8]$; 4) $[0{,}4]$; 5) $\left[-3\frac{1}{2}\right]$; 6) $[-2, 3]$; 7)* $[\sqrt{13}]$; 8) $[\sqrt{25}]$; 9)* $[\sqrt[3]{30}]$; 10) $[\sqrt[4]{200}]$;

11)* $[\sqrt{715}+1]$; 12) $[\sqrt[4]{580}+1]$; 13)* $\left[\frac{\sqrt{542}+2}{3}\right]$;

14) $\left[4+\cos\frac{101\pi}{204}\right]$; 15)* $\left[\frac{17}{8}+\sin 1^\circ\right]$; 16) $[2+\lg 0{,}3]$;

17)* $[1+\lg 12{,}5]$; 18) $[2-\lg 2512]$; 19)* $[1+\ln 5]$;

20) $[1-\ln 50]$.

60. Показать, что $[x+y] \geqslant [x]+[y]$ для любых вещественных x и y.

61. Решить уравнение $[ax]=m$, где $a \neq 0$ и x — вещественное число.

62. Найти, при каком целом положительном m

$$[12{,}4 \cdot m] = 86.$$

63. Показать, что если θ — вещественное число, удовлетворяющее условию $0 \leqslant \theta < 1$, то $[\theta]+\left[\theta+\frac{1}{2}\right]=[2\theta]$.

64. Путешественник был в пути целое число дней и проезжал каждый день столько километров, сколько всего дней был в пути. Если бы он проезжал каждый день по 20 *км* и останавливался на один день через каждые 40 *км*, то время его путешествия увеличилось бы на 37 дней. Определить, сколько всего дней путешественник был в пути.

65. Найти показатель степени числа 3 в каноническом разложении числа 100!.

66. Найти показатель степени числа 11 в каноническом разложении числа 1000!.

67. Сколькими нулями оканчивается число 100!?

68. Разложить на простые множители числа: 1) 10!; 2) 15!; 3) 20!; 4) 25!; 5) 30!.

69. Найти количество целых положительных чисел, не превосходящих 180 и не делящихся ни на одно из простых чисел 5, 7, 11.

70. Найти количество целых положительных чисел, не превосходящих 2311 и не делящихся ни на одно из чисел 5, 7, 13, 17.

71. Найти количество целых положительных чисел, не превосходящих 100 и взаимно простых с числом 36.

72. Найти количество целых положительных чисел, не превосходящих 12 317 и взаимно простых с числом 1575.

73. Найти количество целых положительных чисел, не превосходящих 1000 и не взаимно простых с числом 363.

74. В ряду натуральных чисел 1, 2, 3, . . . , 1800, начиная с 1, вычеркивается каждое пятое число, каждое восьмое и каждое девятое. Сколько чисел не будет вычеркнуто?

75. Доказать, что $\pi(x) = B(x; 2, 3, \ldots, p) + k - 1$, где 2, 3, . . . , p есть k последовательных простых чисел, не превосходящих $\sqrt{x}$. Пользуясь результатом этой задачи, найти $\pi(100)$.

76. Дано, что $B(x; p_1, p_2, \ldots, p_k) = a$. Найти x, если x — число, кратное простым числам $p_1, p_2, \ldots, p_k$.

77. Сколько чисел в интервале от 1 до 120 делится на одно и только одно какое-нибудь из чисел 2, 3 или 5?

78. В урне находится 5000 шаров, перенумерованных от 1 до 5000. Как велика вероятность того, что вынутый наудачу шар будет иметь номер, кратный какому-нибудь из чисел 14, 21, 10?

79. Доказать, что наибольший показатель, с которым простое нечетное число p входит в каноническое разложение $1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2m+1)$, равен:

$$\left[\frac{2m+1}{p}\right] - \left[\frac{m}{p}\right] + \left[\frac{2m+1}{p^2}\right] - \left[\frac{m}{p^2}\right] + \ldots + \left[\frac{2m+1}{p^k}\right] - \left[\frac{m}{p^k}\right],$$

причем

$$p^k \leqslant 2m+1 < p^{k+1}.$$

80. Найти число целых и положительных решений уравнения

$$\left[\frac{x}{a}\right] = \left[\frac{x}{a-1}\right],$$

где $a > 1$ — целое положительное число.

81. Если x—число действительное и n—натуральное, то

$$[x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \ldots + \left[x + \frac{n-1}{n}\right] = [nx].$$

§ 6. Функция $\{x\}$

Функция $\{x\}$ определяется для всех вещественных x и представляет собой *дробную часть* от x. Эта функция находится по формуле:

$$\{x\} = x - [x].$$

82. Найти: 1) $\{2,6\}$, 2) $\left\{\frac{8}{3}\right\}$, 3) $\{7\}$, 4) $\{-4,35\}$, 5)* $\{0,4\}$, 6) $\left\{-2\frac{1}{2}\right\}$, 7)* $\{-4,8\}$, 8)* $\{-0,5\}$.

§ 7. Функции $\sigma(a)$ и $\tau(a)$

Функции $\sigma(a)$ и $\tau(a)$ определяются для всех натуральных a и представляют собой соответственно *сумму и число всех натуральных делителей* данного натурального числа a. Вычисляются эти функции по формулам:

$$\sigma(a) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdots \frac{p_n^{\alpha_n+1}-1}{p_n-1};$$

$$\tau(a) = (\alpha_1+1)(\alpha_2+1) \ldots (\alpha_n+1),$$

где $p_1, p_2, \ldots, p_n$ — простые делители числа a и $\alpha_1, \alpha_2, \ldots, \alpha_n$ — показатели степеней простых делителей в каноническом разложении числа a:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}.$$

---

83. Найти сумму и число всех натуральных делителей следующих чисел: 1) 375; 2) 720; 3) 957; 4) 988; 5) 990; 6) 1200; 7)* 1440; 8)* 1500; 9)* 1890; 10)* 4320.

84. Найти все делители чисел: 1) 360, 2) 375, 3)* 957, 4)* 988.

85. Найти целое положительное число, зная, что оно имеет только два простых делителя, число всех делителей равно 6, а сумма всех делителей равна 28.

86. $N = p^\alpha q^\beta$, где p и $q \neq p$ — простые числа. N^2 имеет 15 различных делителей. Сколько делителей имеет N^3?

87. Вывести формулу суммы k-х степеней всех делителей числа $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$.

88. Пользуясь выведенной формулой, найти:

1) $\sigma_2(12)$, 2) $\sigma_2(18)$, 3)* $\sigma_3(36)$, 4) $\sigma_2(16)$, 5)* $\sigma_3(8)$.

89. Показать, что числа 28, 496, 8128 являются совершенными, т. е. равными полусумме всех своих делителей.

90. Показать, что произведение всех делителей числа N равно $N^{\frac{n}{2}}$, где n — число всех его делителей.

91. Найти число N, произведение всех делителей которого равно 5832.

92. Найти число N, произведение всех делителей которого равно $3^{30} \cdot 5^{40}$.

93. Доказать, что

$$N = \frac{d_1 + d_2 + \ldots + d_{n-1} + d_n}{\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_{n-1}} + \frac{1}{d_n}},$$

где $d_1, d_2, \ldots, d_n$ — все делители числа N.

94. Сколько существует различных разложений на два множителя числа, данного каноническим разложением $N = a^\alpha b^\beta \ldots m^\mu$ ($a, b, \ldots, m$ — простые числа)?

95. Найти число $N = 2^\alpha \cdot 5^\beta \cdot 7^\gamma$, зная, что $5N$ имеет на 8 делителей больше, чем N; $7N$ — на 12 делителей больше, чем N; $8N$ — на 18 делителей больше, чем N.

96. Число N имеет вид:

$$N = 2^x \cdot 3^y \cdot 5^z.$$

Если N разделить на 2, то новое число будет иметь на 30 делителей меньше, чем N; если N разделить на 3, то новое число будет иметь на 35 делителей меньше, чем N; если N разделить на 5, то делителей будет меньше на 42. Найти N.

§ 8. Функция Эйлера $\varphi(a)$

Функция Эйлера $\varphi(a)$ определяется для всех натуральных a и представляет собой количество натуральных чисел, взаимно простых с a и не превосходящих a; при этом считается, что $\varphi(1) = 1$. Вычисляется эта функция по формуле:

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right),$$

где $p_1, p_2, \ldots, p_n$ — простые делители в каноническом разложении

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}.$$

В частности, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ и $\varphi(p) = p - 1$.

Функция Эйлера мультипликативна, т. е.

$$\varphi(a \cdot b \cdot \ldots \cdot l) = \varphi(a) \cdot \varphi(b) \cdot \ldots \cdot \varphi(l)$$

при попарно простых $a, b, \ldots, l$.

97. Найти функцию Эйлера для чисел: 1) 375; 2) 720; 3)* 957; 4) 988; 5)* 990; 6) 1200; 7)* 1440; 8) 1500; 9)* 1890; 10) 4320.

98. Найти функцию Эйлера для простых чисел:
1) 17; 2) 31; 3)* 43; 4) 71; 5)* 83.

99. Найти функцию Эйлера для степеней простых чисел: 1) 3^5; 2) 5^4; 3)* 11^3; 4) 17^2; 5)* 23^2.

100. Найти функцию Эйлера от каждого из следующих произведений, не вычисляя самих произведений: 1) $5 \cdot 11$; 2) $5 \cdot 7 \cdot 13$; 3)* $17 \cdot 23$; 4) $12 \cdot 17$; 5)* $14 \cdot 15$; 6) $11 \cdot 14 \cdot 15$; 7)* $32 \cdot 81 \cdot 49$; 8)* $24 \cdot 28 \cdot 45$; 9)* $720 \cdot 957$; 10) $990 \cdot 1890$.

Указание. Чтобы сомножители были попарно простыми, следует предварительно представить их, а затем и все произведение в каноническом разложении. Например, $12 \cdot 21 \cdot 28 = 2^2 \cdot 3 \cdot 3 \cdot 7 \cdot 2^2 \cdot 7 = 2^4 \cdot 3^2 \cdot 7^2$.

101. Сколько чисел в интервале от 1 до 120 не взаимно простых с 30?

102. Дано, что $\varphi(a) = 3600$ и $a = 3^\alpha \cdot 5^\beta \cdot 7^\gamma$. Найти a.

103. Дано, что $\varphi(a) = 120$ и $a = pq$, где p и q — различные простые числа. Найти a, если $p - q = 2$.

104. Дано, что $\varphi(a) = 11\,424$ и $a = p^2q^2$, где p и q — различные простые числа. Найти a.

105. Найти a, если $\varphi(a) = 462\,000$ и $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ с показателями $\alpha_1, \alpha_2, \dots, \alpha_n$, большими единицы.

106. Показать, что сумма (S) чисел, взаимно простых с числом m и меньших m, вычисляется по формуле:

$$S = \frac{1}{2} m \cdot \varphi(m).$$

107. Применить формулу $S = \frac{1}{2} m \cdot \varphi(m)$ для чисел:
1) 12; 2)* 15; 3) 18; 4)* 28; 5) 375; 6)* 720.

108. Решить уравнение $\varphi(7^x) = 705\,894$.

109. Сколько существует положительных правильных несократимых дробей $\frac{a}{b}$ с данным знаменателем b?

110. На основании решения предыдущей задачи найти количество всех положительных правильных несократимых дробей со знаменателями: 1) 10; 2) 16; 3) 36; 4)* 17; 5) 72.

111. Найти число всех положительных правильных несократимых дробей $\frac{a}{b}$ со знаменателями от $b = 2$ до $b = n$.

112. На основании решения предыдущей задачи найти число всех положительных правильных несократимых дробей со знаменателями: 1) от 2 до 5; 2) от 2 до 10; 3) от 2 до 15.

113. Найти количество натуральных чисел, меньших числа 300 и имеющих с ним наибольшим общим делителем число 20.

114. Найти количество натуральных чисел, меньших числа 1665 и имеющих с ним наибольшим общим делителем число 37.

115. Найти количество натуральных чисел, меньших числа 1476 и имеющих с ним наибольшим общим делителем число 41.

116. Доказать, что при $m \geqslant 3$ значение $\varphi(m)$ есть всегда число четное.

117. Проверить справедливость формулы Гаусса

$$\sum_{d/a} \varphi(d) = a$$

для следующих значений числа a: 1) 72; 2)* 80; 3)* 360; 4)* 375; 5)* 957; 6)* 2800.

118. Доказать, что

$$\varphi(4n) = 2\varphi(2n), \quad \varphi(4n+2) = \varphi(2n+1).$$

119. Найти x, если $\varphi(x) = 12$.

120. Решить уравнение: $\varphi(2x) = \varphi(3x)$.

121. Доказать, что уравнение $\varphi(5x) = \varphi(7x)$ неразрешимо в целых числах.

122. Показать, что если $\varphi(m) = 2^\beta \cdot 3$ и $m = p_1 p_2 \ldots p_k$, где p_i — различные простые нечетные числа, то $p_i = 2^{\alpha_i} \times \times 3 + 1$ или $p_i = 2^{\alpha_i} + 1$, где $\alpha_i > 0 (i = 1, 2, \ldots, k)$.

123. Найти x, если: 1) $\varphi(x) = \frac{1}{2}x$, 2) $\varphi(x) = \frac{2}{3}x$, 3) $\varphi(x) = \frac{1}{3}x$, 4) $\varphi(x) = \frac{1}{4}x$.

ГЛАВА III

СРАВНЕНИЯ

§ 9. Понятия о сравнениях и свойства сравнений

О п р е д е л е н и е с р а в н е н и я. Два целых числа a и b, дающие при делении на целое положительное число m один и тот же остаток:

$$a = mq_1 + r \text{ и } b = mq_2 + r,$$

называются *равноостаточными* или *сравнимыми* между собой по модулю m, что записывается так:

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

и читается: «a сравнимо с b по модулю m».

Т е о р е м а (о смысле сравнения). *Если* $a \equiv b \pmod{m}$, *то разность* $a - b$ *делится на* m, *и наоборот, если разность между двумя числами* a *и* b *делится на* m, *то* $a \equiv b \pmod{m}$.

С л е д с т в и е. *Всякое целое число сравнимо со своим остатком по любому модулю* m, т. е. если

$$a = mq + r,$$

то

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

В частности, если $r = 0$, то $a \equiv 0 \pmod{m}$; это сравнение показывает, что m/a и, наоборот, если m/a, то пишут $a \equiv 0 \pmod{m}$.

О с н о в н ы е с в о й с т в а с р а в н е н и й (аналогичные свойствам равенств).

1. *Два целых числа, сравнимые с третьим по общему модулю, сравнимы между собой*, т. е. если

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

то

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

2. *Сравнения с общим модулем можно почленно складывать и вычитать*, т. е. если

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m},$$

то

$$a \pm c \equiv b \pm d \pmod{m}.$$

Следствия.

1) *Члены сравнения можно переносить из одной части в другую с противоположным знаком*, т. е. если, например,

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

то

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

2) *К одной части сравнения можно прибавлять или вычитать из нее любое число, кратное модулю*, т. е. если

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

то

$$a \pm mk \equiv b \pmod{m}, \text{ или } a \equiv b \pm mk \pmod{m}.$$

3. *Сравнения с общим модулем можно почленно перемножать*, т. е. если

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m},$$

то

$$ac \equiv bd \pmod{m}.$$

Это свойство распространяется и на случай n сравнений.

Следствия. 1) *Обе части сравнения можно возвышать в степень с целым положительным показателем*, т. е. если

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

то

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

2) *Обе части сравнения можно умножать на одно и то же целое число*, т. е. если

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

то

$$ak \equiv bk \pmod{m}.$$

4. *Обе части сравнения можно делить на их общий делитель, если он взаимно прост с модулем* m, т. е. если

$$ak \equiv bk \pmod{m} \text{ и } (k, m) = 1,$$

то

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

5. *Если* $f(x)$ *есть целая рациональная функция с целыми коэффициентами*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

и если

$$x \equiv x_1 \pmod{m},$$

то

$$f(x) \equiv f(x_1) \pmod{m}.$$

Особые свойства сравнений.

1. *Обе части сравнения и модуль можно умножать на одно и то же целое положительное число*, т. е. если

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

то

$$ak \equiv bk \pmod{mk}.$$

2. *Обе части сравнения и модуль можно делить на любой их общий делитель*, т. е. если

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

и

$$a = a_1d, \quad b = b_1d, \quad m = m_1d,$$

то

$$a_1 \equiv b_1 \pmod{m_1}.$$

3. *Если сравнение имеет место по нескольким модулям, то оно имеет место по модулю, равному наименьшему общему кратному данных модулей*, т. е. если

$$a \equiv b \pmod{m_1}, \; a \equiv b \pmod{m_2}, \; \ldots, \; a \equiv b \pmod{m_k},$$

то

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

где $M = [m_1, m_2, \ldots, m_k]$.

4. *Если сравнение имеет место по модулю* m, *то оно имеет место и по модулю* d, *равному любому натуральному делителю числа* m.

5. *Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения делится на это число.*

---

124. Показать, что если n — нечетное число, то $n^2 - 1 \equiv 0 \pmod{8}$.

125. Если p — простое число, то $(a+b)^p \equiv a^p + b^p \pmod{p}$.

126. Показать, что если $100a + 10b + c \equiv 0 \pmod{21}$, то

$$a - 2b + 4c \equiv 0 \pmod{21}.$$

127. Если $3^n \equiv -1 \pmod{10}$, то $3^{n+4} \equiv -1 \pmod{10}$.

128. Показать, что $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$.

129. С каким наименьшим по абсолютной величине числом сравнимо число $N = 11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$ по модулю 7?

130. Проверить, что $3^{14} \equiv -1 \pmod{29}$.

131. Найти остаток от деления $1532^5 - 1$ на 9.

132. Доказать, что если p — простое число, то

$$C_{p-1}^{k} \equiv (-1)^k \pmod{p}.$$

133. По утверждению Ферма, $2^{2^n} + 1$ — простое число при всех натуральных n. Эйлер показал, что уже при $n = 5$ получается число, кратное 641. Проверить.

134. Доказать, что если даны два сравнения

$$\left.\begin{aligned} ac &\equiv bd, \\ a &\equiv b \end{aligned}\right\} \pmod{m}$$

и $(a, m) = 1$, то можно почленно первое сравнение разделить на второе и написать

$$c \equiv d \pmod{m}.$$

135. Известно, что $a^{100} \equiv 2 \pmod{73}$ и $a^{101} \equiv 69 \pmod{73}$. Найти остаток от деления числа a на 73.

136. Дано, что выражение $\dfrac{11a + 2b}{19}$ есть целое число. Доказать, что тогда и $\dfrac{18a + 5b}{19}$ тоже целое число.

137. Доказать, что

$$1^{2k+1} + 2^{2k+1} + 3^{2k+1} + \ldots + (p-1)^{2k+1} \equiv 0 \pmod{p},$$

где p — простое число, большее 2.

138. Доказать, что если $a \equiv b \pmod{p^n}$, то $a^p \equiv b^p \pmod{p^{n+1}}$ (p — число простое).

§ 10. Вычеты и системы вычетов

Совокупность целых чисел, дающих при делении на натуральное число m (модуль) один и тот же остаток r, образует *класс чисел* по этому модулю m. Все числа данного класса в общем виде записываются так: $mk + r$, где k — любое целое число. Число всех классов равно m.

Любое число класса называется *вычетом* по данному модулю m (по отношению ко всем числам того же класса).

Совокупность любых чисел, взятых из каждого класса по одному, называется *полной системой вычетов* по данному модулю m.

Обычно в качестве полной системы вычетов употребляется *полная система наименьших неотрицательных вычетов* по данному модулю m, т. е. система чисел: $0, 1, 2, \ldots, m-1$.

Иногда употребляется и *полная система наименьших по абсолютной величине неположительных вычетов* по данному модулю m, т. е. числа: $-(m-1), -(m-2), \ldots \ldots, -2, -1, 0$.

Часто употребляется также *полная система абсолютно наименьших вычетов* по модулю m. Например, для $m = 5$ этой системой будут числа: $-2, -1, 0, 1, 2$; для $m = 6$ — числа: $-2, -1, 0, 1, 2, 3$ или $-3, -2, -1, 0, 1, 2$.

Совокупность чисел, взятых из полной системы вычетов и взаимно простых с модулем m, называется *приведенной системой вычетов* по этому модулю m. Число чисел, составляющих приведенную систему вычетов, равно $\varphi(m)$.

Употребляются те же три вида приведенной системы вычетов, что и полной системы, но теперь они носят названия: *приведенная система наименьших положительных вычетов, приведенная система наименьших по абсолютной величине отрицательных вычетов и приведенная система абсолютно наименьших вычетов.*

По простому модулю p приведенная система наименьших вычетов отличается от полной системы только отсутствием вычета нуль и состоит из чисел:

$1, 2, 3, \ldots, p-1$ — приведенная система наименьших положительных вычетов;

$-(p-1), -(p-2), \ldots, -2, -1$ — приведенная система наименьших по абсолютной величине отрицательных вычетов.

$\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$ — приведенная система абсолютно наименьших вычетов

Общее свойство полной и приведенной системы вычетов.

Если числа $x_1, x_2, \ldots, x_s$ представляют собой полную ($s = m$) или приведенную ($s = \varphi(m)$) систему вычетов по

модулю m, то и числа $ax_1, ax_2, \ldots, ax_s$, где $(a, m) = 1$, также представляют собой соответственно полную или приведенную систему вычетов по модулю m.

---

139. Написать все три вида как полной, так и приведенной системы вычетов по следующим модулям: 1) $m = 9$; 2) $m=8$; 3)* $p = 13$; 4)* $m = 12$; 5)* $m = 15$; 6)* $p = 7$; 7)* $m = 10$.

140. Показать, что числа 25, —20, 16, 46, —21, 18, 37, —17 составляют полную систему вычетов по модулю $m = 8$.

141*. Показать, что числа 32, —9, 15, 42, —18, 30, 6 составляют полную систему вычетов по модулю $p = 7$.

142*. Показать, что числа 21, 2, —18, 28, —19, 40, —22, —2, 15 составляют полную систему вычетов по модулю $m = 9$.

143*. Показать, что числа 24, 18, —19, 37, 28, —23, —32, 5, 41, —35, —33 составляют полную систему вычетов по модулю $m = 11$.

144*. Показать, что числа 19, 23, 25, —19 составляют приведенную систему вычетов по модулю $m = 12$.

145*. Показать, что числа 11, —1, 17, —19 составляют приведенную систему вычетов по модулю $m = 8$.

146*. Показать, что числа 13, —13, 29, —9 составляют приведенную систему вычетов по модулю $m = 10$.

147. Найти наименьшие неотрицательные, наименьшие по абсолютной величине неположительные и абсолютно наименьшие вычеты чисел 24, 14, 25, 37, —8, —19, —40 по модулю $m=6$. Ко скольким различным классам принадлежат данные числа по данному модулю? Какие числа из данных принадлежат к одному и тому же классу по данному модулю?

148*. Условие предыдущей задачи применить к числам 17, —14, 19, —49, —22, 21, —29 по модулю $m = 8$.

149. Найти наименьшие неотрицательные, наименьшие по абсолютной величине неположительные и абсолютно наименьшие вычеты числа 100 по модулям: 5, 7, 11, 25, 120, 200.

150*. Условие предыдущей задачи применить к числу 50 по модулям: 3, 8, 12, 25, 70, 100.

151*. Заменить вычеты —9, —8, —7, —6, —5, —4, —3, —2, —1, 0 по модулю 10 наименьшими неотрицательными вычетами по этому модулю.

§ 11. Теоремы Эйлера и Ферма

Теорема Эйлера. *При* $m > 1$ *и* $(a, m) = 1$ *имеет место сравнение*:

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

где $\varphi(m)$ *— функция Эйлера.*

Теорема Ферма. *При* p *простом и* $(a, p) = 1$ *имеет место сравнение*:

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

Следствие.

$$a^p - a \equiv 0 \pmod{p}$$

при любом целом положительном a.

---

152. Проверить теорему Эйлера: 1) при $a = 5$, $m = 24$; 2)* при $a = 2$, $m = 33$; 3)* при $a = 3$, $m = 16$; 4) при $a = 3$, $m = 18$; 5)* при $a = 3$, $m = 24$.

153. Пользуясь теоремами Эйлера и Ферма, составить сравнения по модулям: 1) 6; 2) 5; 3)* 8; 4)* 7; 5)* 10; 6)* 12. Выписать значения a и классы чисел, удовлетворяющих каждому сравнению.

154. Найти остатки от деления: 1) 383^{175} на 45; 2) 109^{345} на 14; 3) 439^{291} на 60; 4) 293^{275} на 48; 5)* 66^{17} на 7; 6)* 117^{53} на 11.

155. Найти остатки от деления: 1) $3^{80} + 7^{80}$ на 11; 2) $3^{100} + 5^{100}$ на 7; 3) $2^{100} + 3^{100}$ на 5; 4) $5^{70} + 7^{50}$ на 12; 5)* $5^{80} + 7^{100}$ на 13; 6)* $5^{50} + 13^{100}$ на 18.

156. Найти последние две цифры числа 2^{100}.

157. Найти последние три цифры числа 243^{402}.

158. Найти остаток от деления 93^{41} на 111.

159. Доказать, что если $a^p \equiv \pm 1 \pmod{p}$, то тогда и $a^p \equiv \pm 1 \pmod{p^2}$ (p — число простое).

160. Если p и q — неравные между собой простые числа, то

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

161. Доказать, что при любом целом x

$$x^7 \equiv x \pmod{42}.$$

162. Показать, что если $m > 1$ — нечетное число, то $2^{\varphi(m)-1}$ дает при делении на m остаток, равный $m - \left[\frac{m}{2}\right]$.

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

164. Доказать, что если $N = a_1 + a_2 + \ldots + a_n$ делится на 30 (a_i — целые и положительные числа), то и

$$M = a_1^5 + a_2^5 + \ldots + a_n^5$$

делится на 30.

165. Показать, что 100-я степень любого целого числа либо делится на 125, либо при делении на 125 дает остаток, равный 1.

166. Показать, что если $(a, 10) = 1$, то $a^{100n+1} \equiv a \pmod{1000}$, где n — натуральное число.

167. Показать, что $2^{19 \cdot 73-1} \equiv 1 \pmod{19 \cdot 73}$.

168. Показать, что сравнение

$$a^{6m} + a^{6n} \equiv 0 \pmod 7,$$

где m и n — натуральные числа, может иметь место только при a, кратном 7.

169. Показать, что если $(n, 6) = 1$, то $n^2 \equiv 1 \pmod{24}$.

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

171. Найти простое число p из условия:

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

172. Показать, что произведение трех последовательных целых чисел, среднее из которых равно кубу некоторого целого числа, делится на 504.

173. Показать, что если при $p > 3$ числа p и $2p + 1$ — простые, то $4p + 1$ — число составное.

§ 12. Сравнения с одним неизвестным (общие понятия)

Сравнение n-й степени с одним неизвестным в общем виде записывается так:

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod m,$$

или короче

$$f(x) \equiv 0 \pmod m,$$

где коэффициенты $a_0, a_1, \ldots, a_n$ — целые числа и показатель n степени сравнения — целое неотрицательное число.

Решить сравнение — значит найти все значения x, удовлетворяющие сравнению.

Два сравнения по одному и тому же модулю с одним и тем же неизвестным x называются *равносильными*, если им удовлетворяют одни и те же значения x.

Если сравнению $f(x) \equiv 0 \pmod{m}$ удовлетворяет какое-либо значение $x = \alpha$, то этому сравнению удовлетворяют и все числа, сравнимые с α по модулю m: $x \equiv \alpha \pmod{m}$, или, что то же, $x = mk + \alpha$, т. е. все числа, составляющие *один класс вычетов* по модулю m, которому принадлежит α. Каждый класс составляет одно решение. Следовательно, *решить сравнение* — значит найти *классы чисел*, удовлетворяющих сравнению.

Так как числа, взятые из каждого класса по одному, составляют полную систему вычетов, то найти классы чисел, удовлетворяющих данному сравнению, это значит найти соответствующие им вычеты полной системы, удовлетворяющие сравнению. Обычно в качестве α берутся *наименьшие неотрицательные* или *абсолютно наименьшие вычеты* по данному модулю m. Таким образом, *сколько вычетов из этой системы удовлетворяют сравнению, столько решений и имеет сравнение.*

---

174. Путем испытаний наименьших неотрицательных вычетов найти решения следующих сравнений:

1) $5x^2 - 15x + 22 \equiv 0 \pmod{3}$;
2) $x^2 + 2x + 2 \equiv 0 \pmod{5}$;
3) $3x \equiv 1 \pmod{5}$;
4)* $3x \equiv 1 \pmod{13}$;
5) $8x \equiv 3 \pmod{14}$;
6)* $2x \equiv 7 \pmod{15}$;
7)* $6x \equiv 5 \pmod{9}$;
8)* $x^3 - 2x + 2 \equiv 0 \pmod{3}$;
9) $x^3 - 2 \equiv 0 \pmod{5}$;
10)* $2x^3 - 3x^2 + 2x - 1 \equiv 0 \pmod{7}$.

175. Путем испытаний абсолютно наименьших вычетов решить следующие сравнения, предварительно упростив их на основании свойств сравнений:

1) $12x \equiv 1 \pmod{7}$;
2)* $8x \equiv 1 \pmod{5}$;
3) $3x \equiv 13 \pmod{11}$;
4) $6x \equiv 3 \pmod{7}$;
5)* $6x + 5 \equiv 6 \pmod{7}$;
6) $6x + 5 \equiv 1 \pmod{7}$;

7)* $3x + 4 \equiv 2 \pmod 5$;
8)* $15x + 4 \equiv 7 \pmod{11}$;
9) $90x^{20} + 46x^3 - 52x + 46 \equiv 0 \pmod{15}$;
10)* $25x^3 - 36x^2 + 18x + 13 \equiv 0 \pmod{12}$.

176. Применяя второе следствие из второго основного свойства и четвертое основное свойство сравнений, решить сравнения:

1) $2x \equiv 7 \pmod{15}$;
2)* $5x \equiv 2 \pmod 8$;
3)* $7x \equiv 2 \pmod{13}$;
4)* $13x \equiv 5 \pmod{47}$;
5)* $3x \equiv 23 \pmod{37}$.

177. Показать, что если $(n, m) = 1$, то сравнение n-й степени

$$x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod m$$

можно, путем введения нового неизвестного y, привести к сравнению той же степени

$$y^n + b_2y^{n-2} + \ldots + b_n \equiv 0 \pmod m,$$

у которого отсутствует член $(n - 1)$-й степени.

178. Пользуясь предыдущей задачей, привести сравнение

$$x^3 + 5x^2 + 6x - 8 = 0 \pmod{13}$$

к трехчленному виду:

$$y^3 + py + q \equiv 0 \pmod{13}.$$

§ 13. Сравнения первой степени

Сравнение первой степени в общем виде записывается так:

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

При решении сравнения первой степени могут быть следующие три случая:

1) Если $(a, m) = 1$, то сравнение имеет одно и только одно решение (в смысле класса чисел x по модулю m).

2) Если $(a, m) = d > 1$, но свободный член b не делится на d, то сравнение совсем не имеет решений.

3) Если $(a, m) = d > 1$ и b делится на d, то сравнение имеет d решений, которые находятся по формуле

$$x_{k+1} \equiv m_1k + a \pmod m,$$

где $k = 0, 1, 2, \ldots, d-1$; число α — решение сравнения $a_1 x \equiv b_1 \pmod{m_1}$, где $m = m_1 d$. Это сравнение получается из данного $ax \equiv b \pmod{m}$ после сокращения его членов и модуля m на d.

Способы разыскания решения сравнения $ax \equiv b \pmod{m}$ рассматриваются только для первого случая, когда $(a, m) = 1$, так как третий случай сводится к первому после сокращения на d.

Применяются следующие три способа решения:

а) решение находится путем непосредственных испытаний наименьших неотрицательных или абсолютно наименьших вычетов по модулю m;

б) *способ Эйлера*. Решение находится по формуле

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

где $\varphi(m)$ — функция Эйлера;

с) при помощи конечных непрерывных дробей по формуле

$$x \equiv (-1)^n b P_{n-1} \pmod{m},$$

где P_{n-1} — числитель предпоследней подходящей дроби при разложении $\frac{m}{a}$ в непрерывную дробь*.

Замечание. Иногда сравнение легко решается искусственным путем (см. упр. 176).

---

179. Решить способом Эйлера следующие сравнения:

1)* $3x \equiv 1 \pmod{5}$;
2)* $5x \equiv 6 \pmod{7}$;
3) $5x \equiv 7 \pmod{10}$;
4) $3x \equiv 8 \pmod{13}$;
5)* $25x \equiv 15 \pmod{17}$;
6)* $29x \equiv 3 \pmod{12}$;
7)* $5x \equiv 26 \pmod{12}$;
8)* $4x \equiv 7 \pmod{8}$.

Указания. 1) В примерах 5), 6) и 7) сравнения предварительно упростить; 2) правильность ответов проверить подстановкой.

180. Решить при помощи непрерывных дробей следующие сравнения:

---

* Основные сведения из теории конечных непрерывных дробей изложены в § 22 настоящего сборника.

1) $7x \equiv 4 \pmod{19}$;
2)* $13x \equiv 1 \pmod{27}$;
3)* $37x \equiv 25 \pmod{117}$;
4)* $113x \equiv 89 \pmod{311}$;
5)* $221x \equiv 111 \pmod{360}$;
6)* $23x \equiv 667 \pmod{693}$;
7) $143x \equiv 41 \pmod{221}$;
8)* $91x \equiv 143 \pmod{222}$;
9)* $271x \equiv 25 \pmod{119}$;
10) $13x \equiv 178 \pmod{153}$.

Указания. 1) В примерах 8), 9) и 10) сравнения предварительно упростить; 2) правильность ответов проверить подстановкой.

181. Решить одним из способов следующие сравнения, в которых $(a, m) = d > 1$ и $d \mid b$ (третий случай):

1)* $12x \equiv 9 \pmod{15}$;
2) $12x \equiv 9 \pmod{18}$;
3) $20x \equiv 10 \pmod{25}$;
4)* $10x \equiv 25 \pmod{35}$;
5)* $39x \equiv 84 \pmod{93}$;
6)* $90x + 18 \equiv 0 \pmod{138}$;
7)* $375x \equiv 195 \pmod{501}$;
8)* $14x \equiv 22 \pmod{36}$;
9)* $78x \equiv 42 \pmod{51}$;
10)* $114x \equiv 42 \pmod{87}$.

Правильность ответов проверить подстановкой.

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

183*. Приписать справа к числу 32 такие две цифры, чтобы полученное четырехзначное число делилось на 3 и 7.

§ 14. Системы сравнений первой степени

Систему сравнений первой степени с одним и тем же неизвестным, но с разными модулями, запишем в общем виде так:

$$\left.\begin{aligned} a_1x &\equiv b_1 \pmod{m_1},\\ a_2x &\equiv b_2 \pmod{m_2},\\ &\cdots\cdots\cdots\\ a_nx &\equiv b_n \pmod{m_n}. \end{aligned}\right\} \qquad (1)$$

Общий способ (способ последовательного решения) состоит в том, что сначала находится $x \equiv \alpha \pmod{m}$ из первого сравнения, где α — наименьший неотрицательный или абсолютно наименьший вычет по модулю m_1, и берется класс чисел

$$x = m_1t + \alpha, \qquad (*)$$

удовлетворяющих первому сравнению.

Затем это значение x подставляется во второе сравнение, что дает

$$a_2(m_1t + \alpha) \equiv b_2 \pmod{m_2},$$

откуда находится t опять в виде класса чисел

$$t = m_2 t_1 + \beta$$

и подставляется в равенство (*).

В результате получается значение x в виде класса чисел, удовлетворяющих первым двум сравнениям системы. Дальше это значение x подставляется в третье сравнение системы, так же находится t_1, затем находится x и подставляется в четвертое сравнение системы и т. д.

Заметим, что можно идти и несколько иным путем: сначала решается каждое из сравнений системы и представляется в виде:

$$\left.\begin{aligned} x &\equiv \alpha_1 \pmod{m_1}, \\ x &\equiv \alpha_2 \pmod{m_2}, \\ &\cdots\cdots\cdots \\ x &\equiv \alpha_n \pmod{m_n}, \end{aligned}\right\} \tag{2}$$

а затем поступают описанным способом.

Если окажется, что хотя бы одно из сравнений системы (1) не имеет решения или сравнение относительно t_i в описанном способе неразрешимо, то система (1) не имеет решения.

Если для сравнений $a_i x \equiv b_i \pmod{m_i}$ системы (1) $(a_i, m_i) = d_i$ и d_i / b_i, то, сокращая члены и модуль каждого i-го сравнения на d_i, получаем систему:

$$\left.\begin{aligned} \frac{a_1}{d_1} x &\equiv \frac{b_1}{d_1} \left(\mathrm{mod}\, \frac{m_1}{d_1}\right), \\ \frac{a_2}{d_2} x &\equiv \frac{b_2}{d_2} \left(\mathrm{mod}\, \frac{m_2}{d_2}\right), \\ &\cdots\cdots\cdots \\ \frac{a_n}{d_n} x &\equiv \frac{b_n}{d_n} \left(\mathrm{mod}\, \frac{m_n}{d_n}\right), \end{aligned}\right\} \tag{3}$$

эквивалентную (1).

Сравнения этой системы можно решить относительно x и свести решение системы (3) к решению системы:

$$\left.\begin{aligned} x &\equiv \alpha_1 \left(\mathrm{mod}\, \frac{m_1}{d_1}\right), \\ x &\equiv \alpha_2 \left(\mathrm{mod}\, \frac{m_2}{d_2}\right), \\ &\cdots\cdots\cdots \\ x &\equiv \alpha_n \left(\mathrm{mod}\, \frac{m_n}{d_n}\right). \end{aligned}\right\} \tag{4}$$

Если в системе (2) модули $m_1, m_2, \ldots, m_n$ *попарно просты*, то решение ее можно находить не указанным выше общим способом, а по формуле:

$$x_0 = \frac{M}{m_1} y_1 \alpha_1 + \frac{M}{m_2} y_2 \alpha_2 + \ldots + \frac{M}{m_n} y_n \alpha_n,$$

где $M = [m_1, m_2, \ldots, m_n]$ и $y_1, y_2, \ldots, y_n$ есть решения сравнений:

$$\frac{M}{m_i} y_i \equiv 1 \pmod{m_i}.$$

Решением системы будет:

$$x \equiv x_0 \pmod{M}.$$

Этим способом можно решать и систему (4), если модули $\frac{m_1}{d_1}, \frac{m_2}{d_2}, \ldots, \frac{m_n}{d_n}$ попарно просты.

---

184. Решить системы сравнений:

1) $\left.\begin{aligned} x &\equiv 4 \pmod 5, \\ x &\equiv 1 \pmod{12}, \\ x &\equiv 7 \pmod{14}. \end{aligned}\right\}$

2)* $\left.\begin{aligned} x &\equiv 13 \pmod{16}, \\ x &\equiv 3 \pmod{10}, \\ x &\equiv 9 \pmod{14}. \end{aligned}\right\}$

3) $\left.\begin{aligned} x &\equiv 1 \pmod{25}, \\ x &\equiv 2 \pmod 4, \\ x &\equiv 3 \pmod 7, \\ x &\equiv 4 \pmod 9. \end{aligned}\right\}$

4)* $\left.\begin{aligned} 4x &\equiv 3 \pmod 7, \\ 5x &\equiv 4 \pmod{11}, \\ 11x &\equiv 8 \pmod{13}. \end{aligned}\right\}$

5) $\left.\begin{aligned} 2x &\equiv 7 \pmod{13}, \\ 5x &\equiv 8 \pmod{17}, \\ 3x &\equiv 7 \pmod{31}, \\ 14x &\equiv 35 \pmod{19}. \end{aligned}\right\}$

6) $\left.\begin{aligned} 4x &\equiv 7 \pmod{13}, \\ x &\equiv 2 \pmod{17}, \\ 5x &\equiv 3 \pmod 9, \\ 8x &\equiv 4 \pmod{14}. \end{aligned}\right\}$

7) $\left.\begin{aligned} 3x &\equiv 7 \pmod{10}, \\ 2x &\equiv 5 \pmod{15}, \\ 7x &\equiv 5 \pmod{12}. \end{aligned}\right\}$

8) $\left.\begin{aligned} 4x &\equiv 1 \pmod 9, \\ 5x &\equiv 3 \pmod 7, \\ 4x &\equiv 5 \pmod{12}. \end{aligned}\right\}$

9) $\left.\begin{aligned} 5x &\equiv 1 \pmod{12}, \\ 5x &\equiv 2 \pmod 8, \\ 7x &\equiv 3 \pmod{11}. \end{aligned}\right\}$

10) $\left.\begin{aligned} 3x &\equiv 1 \pmod{10}, \\ 4x &\equiv 3 \pmod 5, \\ 2x &\equiv 7 \pmod 9. \end{aligned}\right\}$

185. Найти наименьшее натуральное число, которое при делении на 7, 5, 3, 11 дает соответственно остатки 3, 2, 1, 9.

186. При каких значениях a следующие системы совместны:

1) $\left.\begin{aligned} x &\equiv 5 \pmod{18}, \\ x &\equiv 8 \pmod{21}, \\ x &\equiv a \pmod{35}. \end{aligned}\right\}$ 2) $\begin{aligned} x &\equiv 3 \pmod{11}, \\ x &\equiv 11 \pmod{20}, \\ x &\equiv 1 \pmod{15}, \\ x &\equiv a \pmod{18}? \end{aligned}$

187. Число, записываемое в десятичной системе счисления как $4x\,87y\,6$, делится на 56. Найти это число.

188. Число N, записываемое в десятичной системе счисления как $xyz138$, делится на 7, а $138xyz$ при делении на 13 дает остаток 6 и $x1y3z8$ при делении на 11 дает остаток 5. Найти число N.

189. Найти восьмизначное число, представляющее точный квадрат, зная, что два числа, образуемые одно первыми четырьмя цифрами, а другое остальными четырьмя цифрами, суть числа последовательные.

190. Зная, что число $13xy45z$ делится на 792, найти x, y, z.

191. Найти трехзначные числа, обладающие тем свойством, что, приписав к каждому из них справа следующее за ним, получим точный квадрат.

192. Некоторое целое число при делении на 7 дает в остатке 3; его квадрат при делении на 7^2 дает в остатке 44; наконец, его куб при делении на 7^3 дает в остатке 111. Найти это число.

193. Решить сравнение $x^2 \equiv -1 \pmod{65}$.

§ 15. Решение в целых числах неопределенных уравнений первой степени с двумя неизвестными при помощи сравнений

Неопределенное уравнение первой степени с двумя неизвестными, как известно, имеет вид:

$$ax + by = c,$$

где a, b, c — целые числа.

Если $(a, b) = 1$, то уравнение имеет целые решения, которые в общем виде записываются так:

$$x = x_1 + bt,$$
$$y = y_1 - at$$

или при отрицательном b удобно брать:

$$x = x_1 - bt,$$
$$y = y_1 + at.$$

В этих формулах решения x_1 и y_1 — пара частных целых значений x и y, удовлетворяющих уравнению, и t — произвольное целое число.

Если $(a, b) = d > 1$ и c не делится на d, то уравнение $ax + by = c$ не имеет решений в целых числах.

Из теории неопределенных уравнений первой степени известны несколько способов отыскания пары частных значений неизвестных, удовлетворяющих уравнению.

При помощи сравнений эта пара частных значений находится так: исходя из уравнения $ax + by = c$, записывается сравнение $ax \equiv c \pmod{b}$, где b берется со знаком плюс; значение x, удовлетворяющее сравнению, берется в качестве x_1, а значение y_1 обычно находится непосредственно из уравнения после подстановки в него найденного значения x_1.

---

194. Решить в целых числах уравнения:

1)	$3x + 4y = 13$;	7)*	$53x + 47y = 11$;
2)	$8x - 13y = 63$;	8)	$45x - 37y = 25$;
3)*	$7x - 19y = 23$;	9)	$81x - 48y = 33$;
4)	$39x - 22y = 10$;	10)	$26x + 34y = 13$;
5)*	$17x - 25y = 117$;	11)*	$122x + 129y = 2$;
6)	$43x + 37y = 21$;	12)*	$258x - 172y = 56$.

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

196*. Ставится водопровод протяжением 105 *м*; имеются трубы в 3 *м* и в 4,5 *м* длиной. Сколько нужно поставить тех и других труб?

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

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

§ 16. Сравнения высших степеней по простому модулю

Общий вид таких сравнений следующий:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}, \qquad (1)$$

где p — простое число, $a_0 \not\equiv 0 \pmod{p}$, n — целое неотрицательное число и коэффициенты — целые числа.

Приведем некоторые теоремы из теории сравнений вида (1).

Теорема (о понижении степени сравнения). *Сравнение вида* (1) *при* $n \geqslant p$ *можно заменить равносильным ему сравнением* $R(x) \equiv 0 \pmod{p}$ *степени не выше* $p - 1$, *где* $R(x)$ *представляет собой остаток от деления* $f(x)$ *на* $x^p - x$.

Теорема (о тождественном сравнении). *Если сравнению вида* (1), *где* $n \leqslant p - 1$, *удовлетворяют несравнимые между собой по модулю* p *числа* $\alpha_1, \alpha_2, \ldots, \alpha_k$, *то имеет место тождественное сравнение*:

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_k) f_k(x) \pmod{p}, \qquad (2)$$

или, иначе можно сказать, что *сравнение* (1) *равносильно сравнению*

$$(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_k) f_k(x) \equiv 0 \pmod{p}, \qquad (3)$$

где $f_k(x)$ — многочлен степени $n - k$.

Левую часть сравнения (3) называют также *разложением* $f(x)$ *на множители по данному модулю* p.

Замечание. Разложение многочлена на множители по данному модулю не является алгебраическим разложением по корням уравнения $f(x) = 0$.

Следствие. *Если* $k = n$, *то сравнение* (2) *равносильно сравнению*

$$f(x) \equiv a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) \pmod{p}, \qquad (2')$$

а сравнение (3) — *сравнению*

$$a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) \equiv 0 \pmod{p}. \qquad (3')$$

Теорема (о числе решений). *Сравнение* (1), *где* $n \leqslant p - 1$, *не может иметь больше, чем* n *несравнимых между собой по модулю* p *решений, причем некоторые из них могут оказаться кратными решениями.*

Теорема Вильсона. *Для всякого простого числа* p *имеет место сравнение*

$$(p-1)!+1 \equiv 0 \pmod{p}$$

и наоборот; т. е. *если* $(p-1)!+1$ *делится на* p, *то* p — *число простое.*

---

199. Решить следующие сравнения, предварительно понизив их степени:

1) $6x^{10}-12x+1 \equiv 0 \pmod 5$;
2) $x^5-2x^3+x^2-2 \equiv 0 \pmod 3$;
3)* $x^5-7x^4+9x^2-x+13 \equiv 0 \pmod 3$;
4) $x^7-x^6+5x^2-3 \equiv 0 \pmod 5$;
5)* $x^5+x^4+x^3-x^2-2 \equiv 0 \pmod 5$;
6) $x^7-6 \equiv 0 \pmod 5$;
7)* $x^8+2x^7+x^5-x^4-x+3 \equiv 0 \pmod 5$;
8) $6x^4+17x^2-16 \equiv 0 \pmod 3$;
9)* $4x^7-2x^3+8 \equiv 0 \pmod 5$,
10) $3x^7-2x^6+2x^2+13 \equiv 0 \pmod 5$.

200. Следующие сравнения разложить на множители по данным модулям:

1) $x^3+4x^2-3 \equiv 0 \pmod 5$;
2)* $x^4+x^3-x^2+x-2 \equiv 0 \pmod 5$;
3) $x^4+x+4 \equiv 0 \pmod{11}$;
4)* $x^2+2x+2 \equiv 0 \pmod 5$,
5) $3x^3-1 \equiv 0 \pmod 5$;
6)* $2x^4+x^3-3x^2-2x-2 \equiv 0 \pmod{11}$;
7) $x^4-7x^3+13x^2+21x+23 \equiv 0 \pmod 7$;
8)* $2x^4+x^3-3x^2-2x-2 \equiv 0 \pmod{11}$;
9) $2x^3+5x^2-2x-3 \equiv 0 \pmod 7$;
10) $x^4-2x^2+x+4 \equiv 0 \pmod 7$.

201. Показать, что если p — простое число и $m > p$, то сравнение $x^m \equiv x^{q+r} \pmod p$, где q — частное и r — остаток при делении m на p, имеет место при любом целом значении x, т. е. является тождественным сравнением.

Пользуясь этим сравнением, указать способ понижения степени $n > p$ сравнения

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}$$

при $a_0 \not\equiv 0 \pmod{p}$ до степени, меньшей p.

202. Пользуясь рассмотренным в предыдущей задаче способом, понизить степени следующих сравнений и найти их решения:

1) $8x^{20} - 15x^{19} + 7x^{18} + 28x^{17} - 4x^{16} + 30x^{15} + 10x^6 - 4x^3 + 23x^2 - 21x - 11 \equiv 0 \pmod{13}$;

2) $x^{10} + x^8 + x^7 - x^4 - x^2 + 4x - 3 \equiv 0 \pmod{7}$;

3) $x^{101} + 3x^{15} + x^{11} - 3x^5 + 9x^2 + 10x - 5 \equiv 0 \pmod{11}$;

4) $2x^{35} - 17x^{15} + 13x^8 - 3x^5 + 12x + 5 \equiv 0 \pmod{11}$;

5)* $x^{13} - 2x^7 + x^3 + 1 \equiv 0 \pmod{5}$.

203. Показать, что сравнение $x^3 + ax + b \equiv 0 \pmod{7}$ при $a \not\equiv 0 \pmod{7}$ и $b \not\equiv 0 \pmod{7}$ не имеет трех решений.

204. Найти необходимое и достаточное условие того, чтобы двучленное сравнение по простому модулю p: $x^n \equiv a \pmod{p}$ при $(a, p) = 1$ и $n < p$ имело n решений.

205. Пользуясь выведенным в задаче **204** критерием, выяснить, какие из следующих сравнений вида $x^n \equiv a \pmod{p}$ имеют n решений, и найти эти решения:

1) $x^3 \equiv 1 \pmod{7}$;
2)* $x^2 \equiv 2 \pmod{5}$;
3) $x^5 \equiv 10 \pmod{11}$;
4) $x^4 \equiv 5 \pmod{11}$;
5)* $x^6 \equiv 3 \pmod{7}$;
6)* $x^4 \equiv 3 \pmod{13}$.

206. Показать, что если p — простое число, то $(p - 2)! \equiv 1 \pmod{p}$.

207. Числа p и $p + 2$ являются тогда, и только тогда простыми «близнецами», когда

$$4[(p-1)! + 1] + p \equiv 0 \pmod{p(p+2)}.$$

(Теорема Клемента.)

208. Показать, применяя теорему Вильсона, что сравнению $x^2 \equiv -1 \pmod{p}$, где $p = 4n + 1$, удовлетворяет число $(2n)!$.

§ 17. Сравнения высших степеней по составному модулю

Сравнение

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{m_1 m_2 \ldots m_n}, \quad (1)$$

где $f(x)$ — произвольный многочлен с целыми коэффициентами, $a_0 \not\equiv 0 \pmod{m_1 m_2 \ldots m_n}$, $n > 1$ и $m_1, m_2, \ldots, m_n$ попарно простые, равносильно системе:

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{m_1}, \\ f(x) &\equiv 0 \pmod{m_2}, \\ &\cdots\cdots\cdots \\ f(x) &\equiv 0 \pmod{m_n}. \end{aligned}\right\} \tag{2}$$

Замечание. Число решений сравнения (1) равно произведению числа решений каждого из сравнений системы (2). Если хотя бы одно из сравнений системы (2) не имеет решений, то система несовместна и, следовательно, сравнение (1) не имеет решений.

Сравнение вида

$$f(x) \equiv 0 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}}, \tag{1'}$$

где α_i — целые положительные, а p_i — простые числа, также равносильно системе:

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}}, \\ f(x) &\equiv 0 \pmod{p_2^{\alpha_2}}, \\ &\cdots\cdots\cdots \\ f(x) &\equiv 0 \pmod{p_n^{\alpha_n}}. \end{aligned}\right\} \tag{2'}$$

Решение этой системы сводится к решению сравнений вида

$$f(x) \equiv 0 \pmod{p^{\alpha}}, \tag{3}$$

решение которых, в свою очередь, начинается с решения сравнений

$$f(x) \equiv 0 \pmod{p}. \tag{4}$$

Путем непосредственных испытаний вычетов (лучше абсолютно наименьших) по модулю p находятся все решения сравнения (4). Пусть

$$x \equiv b_1 \pmod{p},$$

или

$$x = pt_1 + b_1 — \tag{5}$$

одно из решений сравнения (4). Для этого решения составляется сравнение

$$\frac{f(b_1)}{p} + f'(b_1)\, t_1 \equiv 0 \pmod{p}$$

($f'(b_1)$ — первая производная функции $f(x)$ при $x = b_1$), из которого находится $t_1 \equiv b_1' \pmod p$, или $t_1 = pt_2 + b_1'$ (при $f'(b_1)$, не делящемся на p). После подстановки значения t_1 в равенство (5) находим:

$$x = p(pt_2 + b_1') + b_1 = p^2t_2 + (pb_1' + b_1) = p^2t_2 + b_2. \quad (6)$$

Далее решается сравнение $\frac{f(b_2)}{p^2} + f'(b_2)\,t_2 \equiv 0 \pmod p$, из которого находим $t_2 \equiv b_2' \pmod p$, или $t_2 = pt_3 + b_2'$, и после подстановки в (6) получим:

$$x = p^2(pt_3 + b_2') + b_2 = p^3t_3 + (p^2b_2' + b_2) = p^3t_3 + b_3. \quad (7)$$

Вычисление продолжаем до тех пор, пока получим $x = p^\alpha t_\alpha + b_\alpha$, или

$$x \equiv b_\alpha \pmod{p^\alpha}. \quad (8)$$

Решение (8) и является решением сравнения (3).

Если окажется, что $f'(b_l)$ делится на p, то решения для t_l не будет, следовательно, и решение (5) не будет решением сравнения (3).

Замечание к решению сравнения (1) и системы (2), понятно, остается в силе и по отношению к решению сравнения (1′) и системы (2′).

---

209. Решить следующие сравнения:

1) $3x^3 + 4x^2 - 7x - 6 \equiv 0 \pmod{15}$;

2) $6x^3 - 3x^2 - 13x - 10 \equiv 0 \pmod{30}$;

3)* $x^4 - 33x^3 + 8x - 26 \equiv 0 \pmod{35}$;

4)* $x^5 - 3x^4 + 5x^3 + 9x^2 + 4x - 12 \equiv 0 \pmod{42}$;

5)* $x^5 + x^4 - 3x^3 + x^2 + 2x - 2 \equiv 0 \pmod{77}$.

210. Решить сравнения:

1) $4x^3 - 8x - 13 \equiv 0 \pmod{27}$;

2)* $x^4 - 3x^3 + 2x^2 - 5x - 10 \equiv 0 \pmod{343}$;

3) $x^4 - 4x^3 + 2x^2 + x + 6 \equiv 0 \pmod{25}$;

4)* $9x^2 + 29x + 62 \equiv 0 \pmod{64}$;

5) $6x^3 - 7x - 11 \equiv 0 \pmod{125}$;

6)* $x^3 + 3x^2 - 5x + 16 \equiv 0 \pmod{125}$;

7)* $x^4 + 4x^3 + 2x^2 + x + 12 \equiv 0 \pmod{625}$.

211. Решить сравнения:

1) $x^4+4x^3+2x^2+x+12\equiv 0 \pmod{45}$;

2) $x^4-3x^3-4x^2-2x-2\equiv 0 \pmod{50}$;

3)* $x^5-5x^4-5x^3+25x^2+4x-20\equiv 0 \pmod{147}$;

4)* $x^5+3x^4-7x^3+4x^2+4x-10\equiv 0 \pmod{175}$;

5)* $x^4-4x^3+2x^2+x+6\equiv 0 \pmod{135}$;

6) $4x^3+7x^2-7x-10\equiv 0 \pmod{225}$;

7)* $31x^4+57x^3+96x+191\equiv 0 \pmod{225}$;

8)* $2x^6-6x^4-7x^2-4\equiv 0 \pmod{441}$;

9)* $2x^6-6x^4-7x^2-4\equiv 0 \pmod{1225}$.

§ 18. Сравнения второй степени, символ Лежандра

Рассмотрим сравнения второй степени вида

$$x^2\equiv a \pmod{p}, \tag{1}$$

где $a\not\equiv 0 \pmod{p}$ и p — нечетное простое число.

Если сравнение (1) разрешимо, то a называется *квадратичным вычетом* по модулю p, в противном случае a называется *квадратичным невычетом* по этому модулю.

Если a — квадратичный вычет по модулю p, то сравнение (1) имеет всегда два различных решения.

Критерий Эйлера. *Число a при $(a, p)=1$ является квадратичным вычетом по модулю p, если имеет место сравнение*

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

если же

$$a^{\frac{p-1}{2}}\equiv -1 \pmod{p}, \tag{3}$$

то a — квадратичный невычет по модулю p.

Символ Лежандра. Сравнения (2) и (3) объединяются в одно сравнение вида

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

где $\left(\frac{a}{p}\right)$ называется *символом Лежандра* и обозначает $+1$ или -1. Число a называется *числителем*, p — *знаменателем* символа Лежандра.

Теперь, если $\left(\frac{a}{p}\right) = 1$, то a — квадратичный вычет по модулю p и сравнение (1) имеет два различных решения; если же $\left(\frac{a}{p}\right) = -1$, то a — квадратичный невычет по модулю p и сравнение (1) неразрешимо.

Символ Лежандра можно находить с помощью критерия Эйлера:

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

но при больших значениях a и p вычисление является громоздким. Вычисление значительно упрощается, если использовать некоторые его свойства:

1. Если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{1}{p}\right) = 1$.
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
4. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
5. $\left(\frac{ab \ldots l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ldots \left(\frac{l}{p}\right)$, где $a, b, \ldots, l$ взаимно просты с p; в частности

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

6. Закон взаимности квадратичных вычетов: *если p и q — различные простые нечетные числа, то*

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

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

---

212. Пользуясь критерием Эйлера, установить, какие числа из приведенной системы наименьших положительных вычетов по модулю 11 являются квадратичными вычетами по этому модулю.

213. Пользуясь критерием Эйлера, найти классы квадратичных вычетов по модулям: 1) 7; 2)* 13; 3)* 17.

214. Решить следующие сравнения путем испытаний абсолютно наименьших вычетов (кроме нуля) по данным модулям:

1) $x^2 \equiv 2 \pmod 7$; 2) $x^2 \equiv 4 \pmod 7$; 3) $x^2 \equiv 3 \pmod 7$;
4)* $x^2 \equiv 3 \pmod{13}$; 5)* $x^2 \equiv 4 \pmod{11}$.

215. Вычислить символы Лежандра:

1) $\left(\frac{63}{131}\right)$; 2)* $\left(\frac{35}{97}\right)$; 3) $\left(\frac{47}{73}\right)$; 4)* $\left(\frac{29}{383}\right)$; 5) $\left(\frac{241}{593}\right)$;
6)* $\left(\frac{257}{571}\right)$; 7) $\left(\frac{251}{577}\right)$; 8)* $\left(\frac{342}{677}\right)$.

216. Вычислением символа Лежандра установить, какие из следующих сравнений разрешимы, и найти их решения:

1) $x^2 \equiv 6 \pmod 7$; 4)* $x^2 \equiv 10 \pmod{13}$;
2)* $x^2 \equiv 3 \pmod{11}$; 5) $x^2 \equiv 5 \pmod{11}$;
3) $x^2 \equiv 12 \pmod{13}$; 6)* $x^2 \equiv 13 \pmod{17}$.

217. Решить следующие сравнения, предварительно приведя их к двучленным сравнениям:

1) $3x^2 + 7x + 8 \equiv 0 \pmod{17}$;

2)* $3x^2 + 4x + 7 \equiv 0 \pmod{31}$;

3) $5x^2 - 11x + 16 \equiv 0 \pmod{41}$;

4)* $12x^2 + 8x - 15 \equiv 0 \pmod{47}$;

5) $5x^2 + x + 4 \equiv 0 \pmod{13}$;

6)* $4x^2 - 11x - 3 \equiv 0 \pmod{23}$.

218. Показать, что если p — простое число вида $4k + 3$ и число a — квадратичный вычет по модулю p, то сравнение $x^2 \equiv a \pmod p$ имеет решения:

$$x \equiv \pm a^{k+1} \pmod p.$$

219. Пользуясь результатом предыдущей задачи, решить сравнения: 1) $x^2 \equiv 2 \pmod{311}$; 2) $x^2 \equiv 3 \pmod{47}$.

220. Показать, что если p — простое число вида $8k + 5$ и a — квадратичный вычет по модулю p, то сравнение $x^2 \equiv a \pmod p$ имеет решения:

$$x \equiv \pm a^{k+1} \cdot 2^{(2k+1)t} \pmod p,$$

где $t = 0$ и 1.

221. Пользуясь результатом предыдущей задачи, решить сравнения: 1) $x^2 \equiv 7 \pmod{29}$; 2) $x^2 \equiv 3 \pmod{37}$.

222. Доказать, что уравнение $11y = 5x^2 - 7$ неразрешимо в целых числах.

223. Произведение двух последовательных целых чисел не может быть сравнимо с 1 по модулю 13.

224. Решить неопределенное уравнение:

$$13y = x^2 - 21x + 110.$$

225. Решить сравнение:

$$5x^2 - 4x - 1 \equiv 0 \pmod{143}.$$

226. Если простое число $p = 8k + 7$, то

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

а если $p = 8k + 3$, то

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

227. Если простое число $p = 4k + 3$, то из чисел a и $-a$ одно является квадратичным вычетом, а другое — невычетом по модулю p; если же $p = 4k + 1$, то либо a и $-a$ — оба квадратичные вычеты, либо оба невычеты.

228. Найти простые числа p, для которых 3 является квадратичным вычетом или невычетом.

ГЛАВА IV

ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

§ 19. Числа, принадлежащие показателю; первообразные корни

Если δ есть наименьшее положительное решение показательного сравнения $a^z \equiv 1 \pmod m$, где $(a, m) = 1$, то число a называется *принадлежащим показателю* δ по модулю m.

Приведем некоторые свойства показателя δ.

1. *Если* $a \equiv b \pmod m$ (при a и b взаимно простых с m), *то числа* a *и* b *принадлежат одному и тому же показателю* δ *по модулю* m.

2. (О кратности показателя z показателю δ.) *Если число* a *принадлежит показателю* δ, *то все значения* z *в сравнении* $a^z \equiv 1 \pmod m$ *есть числа, кратные* δ.

Следствие. Так как по теореме Эйлера $a^{\varphi(m)} \equiv 1 \pmod m$, то показатель δ есть делитель $\varphi(m)$.

3. *Если число* a *принадлежит показателю* δ, *то степени его* $a^0, a^1, a^2, \ldots, a^{\delta-1}$ *несравнимы между собой по модулю* m *и дают все решения сравнения*

$$x^\delta \equiv 1 \pmod m.$$

Если число a принадлежит показателю $\delta = \varphi(m)$, то в этом случае a называется *первообразным корнем* по модулю m.

По составному модулю m в большинстве случаев первообразных корней не существует, так как все значения a в сравнении $a^z \equiv 1 \pmod m$ оказываются принадлежащими показателям δ, меньшим $\varphi(m)$. По простому же модулю p всегда существуют первообразные корни сравнения $x^{p-1} \equiv 1 \pmod p$ — это числа, принадлежащие показателю $\varphi(p) = p - 1$, причем число их равно $\varphi(p-1)$ (теорема Гаусса).

Общий способ отыскания первообразных корней по простому модулю p вытекает из следующей теоремы: *если*

$$g^{\frac{p-1}{p_1}} \not\equiv 1, \quad g^{\frac{p-1}{p_2}} \not\equiv 1, \ldots, g^{\frac{p-1}{p_n}} \not\equiv 1 \pmod{p},$$

где $p_1, p_2, \ldots, p_n$ — *простые делители числа* $p-1$, *то* g *есть первообразный корень сравнения*

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

Для испытаний в качестве g берутся обычно числа $2, 3, \ldots, p-1$ из приведенной системы наименьших положительных вычетов по модулю p (кроме единицы).

Другой способ, менее громоздкий, состоит в следующем: если известен один из первообразных корней (лучше наименьший) g по простому модулю p, то остальные первообразные корни находятся как наименьшие положительные вычеты степеней g^k по модулю p, где $(k, p-1) = 1$ и $1 < k < p-1$.

---

229. Путем испытаний найти показатели, которым принадлежат по модулю m все числа от 2 до $m-1$, взаимно простые с m: 1) $m = 5$; 2)* $m = 7$; 3) $m = 8$; 4)* $m = 10$; 5) $m = 11$; 6)* $m = 9$.

Указание. По следствию из теоремы 2 искомые показатели надо искать среди делителей $\varphi(m)$.

230. Пользуясь общим способом, найти все первообразные корни по модулям: 1) $p = 11$; 2)* $p = 7$; 3) $p = 13$; 4)* $p = 17$.

231. Найти число первообразных корней и наименьший из них по модулям: 1) 19; 2)* 23; 3) 31; 4)* 43; 5) 37; 6)* 53.

232. Зная наименьший первообразный корень по каждому из данных модулей, найти все первообразные корни по этим модулям: 1) 19; 2)* 23; 3)* 31.

233. Показать, что каждый простой делитель числа $2^{2^n}+1$ при $n > 1$ имеет вид $p = k \cdot 2^{n+2} + 1$.

§ 20. Индексы и их применение

Подобно понятию логарифма, в теории сравнений вводится понятие *индекса*, играющего роль логарифма.

Так как степени первообразного корня $g^0, g^1, \ldots, g^{p-2}$ по модулю p образуют приведенную систему поло-

жительных вычетов (только не наименьших) по модулю p, то для всякого числа A, не делящегося на p, непременно будет иметь место сравнение

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

где k — одно из значений 0, 1, 2, . . . , $p-2$.

В этом случае показатель k называется *индексом числа A при основании g по модулю p* и записывается это так:

$$k = \operatorname{ind}_g A,$$

или часто без указания основания: $k = \operatorname{ind} A$.

Свойства индексов

1. *Если* $g^s \equiv g^t \pmod{p}$, *то* $s \equiv t \pmod{p-1}$.
2. $\operatorname{ind} 1 = 0$, так как всегда $1 \equiv g^0 \pmod{p}$.
3. $\operatorname{ind}(AB) \equiv \operatorname{ind} A + \operatorname{ind} B \pmod{p-1}$.
4. $\operatorname{ind} A^n \equiv n \operatorname{ind} A \pmod{p-1}$.
5. $\operatorname{ind} \frac{A}{B} \equiv \operatorname{ind} A - \operatorname{ind} B \pmod{p-1}$.
6. $\operatorname{ind}_g A \equiv \operatorname{ind}_q A \cdot \operatorname{ind}_g q \pmod{p-1}$.

Применение *оперативных* свойств индексов (2—5) будем называть *индексированием*. Индексирование выполняется при помощи таблиц индексов и антииндексов. Для каждого простого модуля p по таблице индексов находятся индексы данных чисел, а по таблице антииндексов находятся числа по данным индексам.

Каждая из таблиц расположена в виде прямоугольника; в заглавной строке стоят цифры 0, 1, 2, . . . , 9; в заглавном столбце цифры 0, 1, 2, . . . ; сначала (для небольших модулей) их немного.

Чтобы найти индекс данного числа, отыскиваются десятки этого числа в заглавном столбце, а единицы — в заглавной строке. На пересечении строки и столбца, идущих от этих десятков и единиц, внутри таблицы и находится искомый индекс данного числа. Аналогично находится и число по данному индексу.

---

234. Составить таблицу индексов: 1) по модулю 29 с основанием 2; 2)* по модулю 23 с основанием 5.

235. Найти показатель δ в сравнениях:

1) $5^{\delta} \equiv 1 \pmod 7$;
2)* $5^{\delta} \equiv 1 \pmod{11}$;
3) $8^{\delta} \equiv 1 \pmod{13}$;
4)* $12^{\delta} \equiv 1 \pmod{17}$;
5) $24^{\delta} \equiv 1 \pmod{31}$;
6)* $10^{\delta} \equiv 1 \pmod{13}$;
7) $27^{\delta} \equiv 1 \pmod{17}$:
8)* $18^{\delta} \equiv 1 \pmod{11}$;
9)* $23^{\delta} \equiv 1 \pmod{41}$.

236. Индексированием найти показатели, которым принадлежат все числа от 2 до $p - 1$ по простым модулям: 1) $p = 5$; 2)* $p = 7$; 3)* $p = 11$.

237. Индексированием установить, являются ли первообразными корнями по модулю 59 следующие числа: 1) 2; 2)* 3; 3) 6; 4)* 8; 5) 12; 6)* 13; 7) 14; 8)* 19.

238. Найти все первообразные корни по следующим модулям: 1) $p = 17$; 2)* $p = 19$; 3)* $p = 23$.

239. Решить показательные сравнения:

1) $2^x \equiv 7 \pmod{67}$;
2)* $13^x \equiv 12 \pmod{47}$;
3) $16^x \equiv 11 \pmod{53}$;
4)* $52^x \equiv 38 \pmod{61}$;
5) $12^x \equiv 17 \pmod{31}$;
6)* $20^x \equiv 21 \pmod{41}$.

240. Решить следующие сравнения первой степени:

1) $7x \equiv 23 \pmod{17}$;
2)* $39x \equiv 84 \pmod{97}$;
3) $125x \equiv 7 \pmod{79}$;
4)* $37x \equiv 25 \pmod{89}$;
5)* $4x \equiv 13 \pmod{37}$;
6) $37x \equiv 5 \pmod{221}$;
7)* $47x \equiv 13 \pmod{667}$;
8)* $228x \equiv 317 \pmod{1517}$.

241. Решить следующие двучленные сравнения:

1) $37x^{15} \equiv 62 \pmod{73}$;
2)* $5x^4 \equiv 3 \pmod{11}$;
3) $2x^8 \equiv 5 \pmod{13}$;
4)* $2x^3 \equiv 17 \pmod{41}$;
5) $27x^5 \equiv 25 \pmod{31}$;
6)* $11x^3 \equiv 6 \pmod{79}$;
7) $23x^3 \equiv 15 \pmod{73}$;
8)* $8x^{26} \equiv 37 \pmod{41}$;
9) $37x^8 \equiv 59 \pmod{61}$;
10)* $18x^8 \equiv 6 \pmod{13}$.

242. Решить следующие двучленные сравнения:

1) $x^{12} \equiv 37 \pmod{41}$;
2)* $x^{55} \equiv 17 \pmod{97}$;
3) $x^{35} \equiv 17 \pmod{67}$;
4)* $x^{30} \equiv 46 \pmod{73}$;
5)* $x^8 \equiv 23 \pmod{41}$;
6)* $x^5 \equiv 74 \pmod{71}$;
7) $x^{27} \equiv 39 \pmod{43}$;
8)* $x^8 \equiv 29 \pmod{13}$;
9) $x^2 \equiv 59 \pmod{67}$:
10)* $x^2 \equiv 59 \pmod{83}$;
11)* $x^2 \equiv 32 \pmod{43}$;
12)* $x^2 \equiv -17 \pmod{53}$;
13) $x^2 \equiv -28 \pmod{67}$;
14)* $x^2 \equiv 56 \pmod{41}$.

243. Пользуясь критерием Эйлера и применением индексов, определить, какие из чисел 15, 16, 17, 18, 19, 20 являются квадратичными вычетами: 1) по модулю 23; 2)* по модулю 29; 3) по модулю 41; 4)* по модулю 73; 5) по модулю 97.

§ 21. Другие приложения теории сравнений

Мы уже видели приложения теории сравнений к ряду задач и примеров (в предыдущих параграфах).

Рассмотрим еще некоторые приложения арифметического характера.

Пользуясь понятием числа, принадлежащего данному показателю, можно определить длину периода при обращении обыкновенной дроби в десятичную периодическую дробь по следующему правилу: *длина периода* (*число цифр в периоде*) *равна наименьшему общему кратному показателей, которым принадлежит число* 10 *по модулям, равным простым множителям* p_1, p_2, p_3, ... *знаменателя, отличным от* 2 *и* 5, *и их степеням* p_1^2, p_2^2, p_3^2, ... *до* $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, $p_3^{\alpha_3}$, ... *включительно, для чего нужно предварительно представить знаменатель в виде* $2^m \cdot 5^n p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

При помощи понятия сравнения можно установить некоторые признаки делимости, которые обычно не рассматриваются в школьном курсе арифметики.

С помощью сравнений можно также проверять правильность выполнения арифметических действий.

---

244. Определить длину периода при обращении следующих обыкновенных дробей в десятичные:

1) $\frac{1}{19}$; 5) $\frac{1}{7 \cdot 23 \cdot 31}$; 8)* $\frac{1}{2 \cdot 11 \cdot 13}$;

2)* $\frac{1}{41}$; 6)* $\frac{1}{11 \cdot 13 \cdot 17}$; 9) $\frac{1}{5 \cdot 2 \cdot 29 \cdot 43}$;

3) $\frac{1}{13 \cdot 37}$; 7) $\frac{1}{5 \cdot 7 \cdot 19}$; 10)* $\frac{1}{4 \cdot 53 \cdot 73}$.

4)* $\frac{1}{17 \cdot 29}$;

245. Установить признак делимости, общий для чисел 7, 11, 13 и для чисел 3, 9, 37.

246. Пользуясь установленными в предыдущей задаче признаками, выяснить:

а) делятся ли числа: 1) 973 126; 2)* 977 132; 3) 96 736 068; 4)* 32 113 158; 5)* 426 297 531; 6)* 385 073 689 на 7, 11 или 13;

б) делятся ли числа: 1) 20 794; 2)* 11 200 122; 3) 2 575 163 на 37.

247. Установить способ проверки результатов арифметических действий при помощи числа 9.

248. Проверить правильность выполнения следующих арифметических действий:

1) $25\,041+91\,382=116\,423$;
2)* $42\,932-18\,265=24\,667$;
3)* $13\,547-9862=3685$;
4) $8264\cdot 5201=42\,981\,064$;
5)* $994\cdot 979=973\,126$;
6)* $3745\cdot 8067=30\,210\,915$;
7) $423\,805\,807:43=9\,855\,949$;
8)* $266\,377:2993=89$;
9)* $28\,342:383=74$.

ГЛАВА V

НЕПРЕРЫВНЫЕ ДРОБИ

§ 22. Конечные непрерывные дроби

Если $\frac{a}{b}$ — обыкновенная несократимая дробь, безразлично правильная или неправильная, то с помощью алгорифма Евклида можно эту дробь представить так:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_n}}}},$$

где q_0—целое неотрицательное число, $q_1, q_2, \ldots, q_n$ — целые положительные числа. Выражение, написанное в правой части, называется *конечной непрерывной* или *цепной* дробью.

Кратко написанное равенство выражается так:

$$\frac{a}{b} = (q_0, q_1, q_2, \ldots, q_n).$$

Числа $q_1, q_2, \ldots, q_n$ называются *знаменателями* непрерывной дроби, а числа $q_0, q_1, q_2, \ldots, q_{n-1}$ — *неполными частными*; все же они $q_0, q_1, q_2, \ldots, q_n$ являются *точными частными* в алгорифме Евклида. Дроби

$$\frac{P_0}{Q_0} = \frac{q_0}{1}, \quad \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1}, \quad \frac{P_2}{Q_2} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}, \ldots$$

$$\ldots, \frac{P_n}{Q_n} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_n}}}$$

называются *подходящими* дробями. Дроби с четными индексами 0, 2, 4, ... называются дробями *четного* порядка, а с нечетными индексами 1, 3, 5, ... — *нечетного* порядка. Очевидно, что

$$\frac{P_n}{Q_n} = \frac{a}{b}.$$

Между подходящими дробями и самой дробью $\frac{a}{b}$ имеют место соотношения:

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

Из этих соотношений видно, что дробь $\frac{a}{b}$ всегда заключена между двумя соседними подходящими дробями, интервал между которыми уменьшается по мере возрастания порядка. Этим и объясняется название «подходящие» дроби.

Между числителями и знаменателями *трех* последовательных подходящих дробей имеет место, начиная с $k = 2$, зависимость:

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

Если условно ввести числа $P_{-2} = 0$, $P_{-1} = 1$, $Q_{-2} = 1$, $Q_{-1} = 0$, то написанное равенство позволяет находить *все* подходящие дроби по следующей схеме:

k	-2	-1	0	1	2	3	$\ldots$	n
q_s	—	—	q_0	q_1	q_2	q_3	$\ldots$	q_n
P_s	0	1	P_0	P_1	P_2	P_3	$\ldots$	P_n
Q_s	1	0	Q_0	Q_1	Q_2	Q_3	$\ldots$	Q_n

Разность между двумя соседними подходящими дробями находится по формуле:

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

Для оценки погрешности при замене дроби $\frac{a}{b}$ подходящей дробью $\frac{P_k}{Q_k}$ будем применять формулу:

$$\left|\frac{a}{b}-\frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_k Q_{k+1}}.$$

---

249. Разложить данную обыкновенную дробь в непрерывную, заменить ее подходящей дробью $\frac{P_4}{Q_4}$, найти погрешность замены, записать замену приближенным равенством с указанием погрешности:

1) $\frac{29}{37}$; 2)* $\frac{163}{159}$; 3) $\frac{648}{385}$; 4) $\frac{571}{359}$; 5)* $\frac{1882}{1651}$; 6)* $\frac{2341}{1721}$.

Указание. В примерах 4) и 6) произвести замену подходящими дробями $\frac{P_5}{Q_5}$.

250. По данным конечным непрерывным дробям найти соответствующие им обыкновенные несократимые дроби:

1) $\frac{a}{b} = (2, 1, 1, 3, 1, 2)$;

2) $\frac{a}{b} = (1, 1, 2, 3, 4)$;

3)* $\frac{a}{b} = (2, 5, 3, 2, 1, 4, 2, 3)$;

4) $\frac{a}{b} = (1, 3, 2, 4, 3, 1, 1, 1, 5)$;

5)* $\frac{a}{b} = (1, 2, 3, 1, 2, 3, 1, 2, 3)$.

251. Сократить с помощью разложения в непрерывную дробь следующие обыкновенные дроби:

1) $\frac{3587}{2743}$; 2)* $\frac{1043}{3427}$; 3) $\frac{3653}{3107}$; 4)* $\frac{11281}{6583}$; 5)* $\frac{11111}{7093}$.

252. Требуется построить зубчатую передачу при помощи двух шестерен с количеством зубцов, равным отношению $\frac{587}{113}$. Можно ли техническое осуществление передачи выполнить заменой заданного отношения количества зубцов шестерен отношением с меньшими числителем и знаменателем, но с погрешностью, не превосходящей 0,001?

253. Найти способ решения неопределенных уравнений первой степени с двумя неизвестными при помощи непрерывных дробей.

254. Пользуясь найденным способом, решить следующие уравнения: 1) $38x + 117y = 209$; 2)* $122x + 129y = 2$; 3) $119x - 68y = 34$; 4)* $258x - 175y = 113$; 5) $41x + 114y = 5$.

§ 23. Бесконечные непрерывные дроби; квадратичные иррациональности

Подобно разложению обыкновенной несократимой дроби в непрерывную, можно любое иррациональное число ω разложить тоже в непрерывную дробь, только бесконечную:

$$\omega = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_k + \cfrac{1}{q_{k+1} + \ddots}}}}},$$

где q_0 — целое число, $q_1, q_2, \ldots, q_k, \ldots$ — целые положительные числа; разложение кратко записывается так:

$$\omega = (q_0, q_1, q_2, \ldots, q_k, \ldots);$$

числа $q_0, q_1, q_2, \ldots, q_k, \ldots$, как и в теории конечных непрерывных дробей, называются по-прежнему *неполными частными*.

Вообще, имеется почти полная аналогия теории бесконечных непрерывных дробей с теорией конечных непрерывных дробей, а именно:

Подходящими дробями по-прежнему будут:

$$\frac{P_0}{Q_0} = \frac{q_0}{1}, \quad \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1}, \quad \frac{P_2}{Q_2} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}, \quad \ldots$$

$$\ldots, \quad \frac{P_k}{Q_k} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_k}}}.$$

Соотношения между подходящими дробями и самим иррациональным числом ω остаются теми же, что и при конечных непрерывных дробях:

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

Сохраняется формула

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

и схема получения подходящих дробей.

По-прежнему имеют место формулы:

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

$$\left|\omega - \frac{P_k}{Q_k}\right| \leqslant \frac{1}{Q_k\, Q_{k+1}}.$$

Разложение иррационального числа ω можно представить еще так:

$$\omega = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{\omega_n}}}}},$$

или, короче,

$$\omega = (q_0,\ q_1,\ q_2,\ \ldots,\ \omega_n),$$

где ω_n называется *полным частным* и снова представляет собой иррациональное число:

$$\omega_n = (q_n,\ q_{n+1},\ \ldots).$$

В этом случае по формуле

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

заменяя неполное частное q_k полным частным ω_n, получаем:

$$\omega = \frac{P_{k-1}\, \omega_n + P_{k-2}}{Q_{k-1}\, \omega_n + Q_{k-2}}.$$

Эта формула выражает ω через полное частное ω_n.

Бесконечные непрерывные дроби могут быть периодическими, как чистыми, так и смешанными.

Бесконечная непрерывная дробь называется *чистой периодической*, если ее неполные частные периодически повторяются в одной и той же последовательности, начиная с q_0, т. е. если дробь имеет вид

$$(q_0, q_1, q_2, \ldots, q_n, q_0, q_1, q_2, \ldots, q_n, \ldots),$$

или в более краткой записи

$$[(q_0, q_1, q_2, \ldots, q_n)].$$

Например (2, 3, 1, 2, 3, 1, 2, 3, 1, . . .), или [(2, 3, 1)].

Если период непрерывной дроби начинается не с q_0, то такая непрерывная дробь называется *смешанной периодической*, т. е. если дробь имеет вид

$$(q_0, q_1, \ldots, q_m, p_0, p_1, \ldots, p_n, p_0, p_1, \ldots, p_n, \ldots),$$

или, короче,

$$[q_0, q_1, \ldots, q_m, (p_0, p_1, \ldots, p_n)].$$

Например (2, 1, 3, 1, 2, 3, 1, 2, 3, 1, 2, . . .), или [2, 1, (3, 1, 2)].

Оказывается, что бесконечные периодические непрерывные дроби, как чистые, так и смешанные, имеют тесную связь с *квадратичными иррациональностями*. Эта связь выражается следующими двумя теоремами:

1. *Всякая бесконечная периодическая непрерывная дробь (чистая или смешанная) есть в е щ е с т в е н н ы й корень квадратного уравнения с целыми коэффициентами, т. е. квадратичная иррациональность.*

2. *Вещественный и р р а ц и о н а л ь н ы й корень всякого квадратного уравнения с целыми коэффициентами разлагается в бесконечную периодическую непрерывную дробь (чистую или смешанную).*

---

255. Следующие квадратичные иррациональности представить непрерывными дробями, заменить каждую подходящей дробью $\frac{P_3}{Q_3}$, найти погрешность замены и записать замену приближенным равенством с указанием погрешности:

1) $\sqrt{11}$; 2)* $\sqrt{10}$; 3) $\sqrt{12}$; 4)* $1+\sqrt{5}$; 5) $1+\sqrt{7}$; 6)* $1+\sqrt{2}$; 7) $\frac{1+\sqrt{3}}{2}$; 8)* $\frac{2+\sqrt{17}}{3}$.

Указание. В примерах 4) и 5) заменить дробью $\frac{P_4}{Q_4}$; в примерах 6), 7) и 8) заменить дробью $\frac{P_k}{Q_k}$ со знаменателем $Q_k > 100$ и ближайшим к 100.

256. Следующие иррациональности представить непрерывными дробями, заменить каждую подходящей дробью с погрешностью не больше 0,0001 и записать замену приближенным равенством с указанием погрешности:

1) $\sqrt{3}$; 2)* $\sqrt{5}$; 3) $\sqrt{6}$; 4)* $\sqrt{13}$; 5) $\frac{2+\sqrt{5}}{3}$;

6)* $\frac{1+\sqrt{7}}{2}$; 7) $\frac{2+\sqrt{14}}{4}$.

257. То же для следующих иррациональностей:

1) $5-\sqrt{15}$; 5) $1-\sqrt{31}$; 9) $-2-\sqrt{17}$;

2)* $7-\sqrt{13}$; 6)* $3-\sqrt{41}$; 10)* $-3-\sqrt{23}$;

3) $\frac{3-\sqrt{7}}{5}$; 7) $\frac{5-\sqrt{37}}{3}$; 11) $\frac{-4-\sqrt{46}}{5}$;

4)* $\frac{5-\sqrt{5}}{2}$; 8)* $\frac{3-\sqrt{29}}{5}$; 12)* $\frac{-5-\sqrt{39}}{2}$.

258. Найти квадратичные иррациональности по их разложениям в периодические непрерывные дроби:

1) [(1, 2, 4, 6)]; 3) [(2, 2, 1, 1)]; 5)* [4, 1, (7, 2, 2)].
2)* [(1, 2)]; 4) [2, (1, 1, 1, 4)];

259. Бо́льшим корнем какого квадратного уравнения с целыми коэффициентами является каждая из следующих периодических непрерывных дробей:

1) [(1, 1, 2, 2, 1)]; 3)* [(1, 4, 2, 3)]; 5)* [2, 5, (1, 2)] ?
2)* [(2, 1)]; 4) [2, (1,1,3)];

260. При помощи непрерывных дробей вычислить с точностью до 0,0001 оба корня каждого из следующих уравнений:

1) $2x^2 - 15x + 26 = 0$; 4)* $3x^2 - 7x - 3 = 0$;
2)* $x^2 + 3x - 5 = 0$; 5) $2x^2 - 3x - 6 = 0$;
3) $x^2 + 9x + 6 = 0$; 6)* $2x^2 + 5x - 4 = 0$.

261. Показать, что непрерывная дробь

$$a+\cfrac{1}{b+\cfrac{1}{a+\cfrac{1}{b+}}}$$
$$\dots,$$

умноженная на непрерывную дробь

$$\cfrac{1}{b+\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{a+}}}}$$
$$\dots,$$

равна $\frac{a}{b}$.

262. Показать, что $\frac{P_2}{Q_2}=\frac{2a+1}{2}$ при разложении иррациональности $\sqrt{a^2+a+1}$ в непрерывную дробь.

263. Разложить $\sqrt{x^2+1}$ в непрерывную дробь и найти $\frac{P_2}{Q_2}$.

§ 24. Алгебраические и трансцендентные числа

Алгебраическими числами называются корни уравнения

$$a_0x^n+a_1x^{n-1}+\dots+a_n=0 \quad (a_0\neq 0), \qquad (1)$$

где показатель степени уравнения n — *натуральное* число, коэффициенты a_0, a_1, ..., a_n — *рациональные* числа.

Очевидно, что в случае рациональных коэффициентов уравнение (1) всегда можно преобразовать в уравнение с целыми коэффициентами.

Алгебраические числа называются *целыми*, если они являются корнями уравнения

$$x^n+a_1x^{n-1}+\dots+a=0 \qquad (2)$$

с целыми рациональными коэффициентами и со старшим коэффициентом a_0, равным единице.

Число α называется алгебраическим числом n-й *степени*, если оно является корнем уравнения (1) степени n

и не является корнем никакого другого уравнения этого вида степени, меньшей n.

Если α и β — алгебраические числа, то $\alpha+\beta$, $\alpha-\beta$ $\alpha\beta$ также являются алгебраическими числами, а если $\beta \neq 0$ то $\frac{\alpha}{\beta}$ — алгебраическое число.

Числа, не являющиеся корнями никакого уравнения вида (1), называются *трансцендентными*. Короче говоря, трансцендентными называются неалгебраические числа.

Теорема Гельфонда. *Всякое число вида* α^{β}, *где* α — *алгебраическое число, отличное от* 0 *и* 1, *и* β — *алгебраическое число не ниже второй степени, трансцендентно.*

---

264. Показать, что следующие числа являются алгебраическими, и определить степень каждого из них:

1) $\frac{3}{5}$; 2)* $2\frac{1}{2}$; 3) $\sqrt{3}$; 4)* $\sqrt[3]{2}$; 5) $1+\sqrt{2}$; 6)* $2-\sqrt{2}$; 7) $2+i$; 8)* $1-2i$; 9) $\sqrt{3}+\sqrt{5}$; 10)* $\sqrt{2}-\sqrt{5}$.

265. Показать, что корни следующих уравнений являются алгебраическими числами степени, равной степени уравнения:

1) $x^3+2x^2-4x+2=0$;
2)* $2x^5+6x^3-9x^2-15=0$;
3)* $x^4-5x^2+10x+20=0$.

266. Показать, что следующие числа являются трансцендентными:

1) $3^{\sqrt{2}}$; 2)* $5^{\sqrt{3}}$; 3) $2^{i\sqrt{3}}$; 4)* 3^{1-i}; 5)* $5^{2-i\sqrt{2}}$.

РЕШЕНИЯ, УКАЗАНИЯ, ОТВЕТЫ

ГЛАВА I

ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ

§ 1. Основные понятия

1. Из условия имеем: $42\,157 = 231\,b + r$, $b = 182 + \dfrac{115 - r}{231}$, отсюда $b = 182$ и $r = 115$.

2. По условию, $\dfrac{mn + pq}{m - p} = t$ — целое число. Возьмем дробь $\dfrac{mq + np}{m - p}$ и вычтем из нее целое число t:

$$\frac{mq + np}{m - p} - t = \frac{mq + np}{m - p} - \frac{mn + pq}{m - p} = \frac{q\,(m-p) - n(m-p)}{m - p} = q - n.$$

Теперь $\dfrac{mq + np}{m - p} = q - n + t$ — целое число.

Следовательно, $mq + np$ делится на $m - p$.

3. По условию, $ad - bc = nt$ и $a - b = nt_1$.

Умножив второе равенство на d и вычтя из результата первое, получим $b(c - d) = n\,(dt_1 - t)$.

Отсюда, учитывая условие относительно чисел b и n, получаем, что $c - d$ делится на n.

4. Дано, что $N = 10^4a + 10^3b + 10^2c + 10d + e$ делится на 41. После круговой перестановки цифр числа (на одну цифру влево) получим число:

$$N_1 = 10^4b + 10^3c + 10^2d + 10e + a = 10\,(10^4a + 10^3b + 10^2c + 10\,d + e) - 10^5a + a = 10N - 99\,999a.$$

Так как $41 \mid N$ и $41 \mid 99\,999$, то $41 \mid N_1$.

5. $m^5 - m = (m-1)m\,(m+1)\,(m^2+1) = (m-1)\,m(m+1)\,[(m^2-4) + 5] = (m-2)\,(m-1)\,m\,(m+1)\,(m+2) + 5\,(m-1)\,(m+1)$.

Каждое слагаемое полученной суммы делится на 30, так как произведение k последовательных чисел натурального ряда делится на $k!$ (это следует из того, что

$$C_n^k = \frac{n\,(n-1)\,(n-2)\ldots(n-k+1)}{1\ 2\ 3\ \ldots\ k}$$ — целое число);

поэтому и сумма делится на 30, а это значит, что $m^5 - m$ делится на 30.

6. Пусть искомое число $10x + 5$. Переставив цифру 5 на первое место слева, получим $5 \cdot 10^5 + x$; в силу условия имеем уравнение $5 \cdot 10^5 + x = 4(10x + 5)$, решая которое, получаем $x = 12\,820$. Искомое число будет 128 205.

7. Произведение, данное в условии, представим так:

$$n(n+1)(2n+1) = n(n+1)[(n-1)+(n+2)] = (n-1)n(n+1) + n(n+1)(n+2).$$

Каждое слагаемое полученной суммы делится на 6 (см. решение задачи 5), следовательно, и сумма делится на 6.

8. Произведение данное в условии, представим так:

$$n(n^2+5) = n[(n^2-1)+6] = n[(n-1)(n+1)+6] = (n-1)n(n+1) + 6n.$$

Теперь ясно, что $n(n^2+5)$ делится на 6.

9. Имеем:

$$\frac{(2m+1)^2-(2n+1)^2}{(2m+1)^2+(2n+1)^2} = \frac{4(m+n+1)(m-n)}{2[2(m^2+n^2+m+n)+1]}.$$

Полученная дробь сократима на 2, но несократима на 4.

10. Имеем: $N^2 = 1000x + 100(y+1) + 10x + y = 101 \cdot (10x+y) + 100$. Отсюда $10x + y = \dfrac{(N+10)(N-10)}{101}$, $N = 91$, $N^2 = 8281$.

11. Чтобы $(n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2 = 5(n^2+2)$ было точным квадратом, нужно, чтобы n^2 было кратно 5, а для этого n^2 должно оканчиваться цифрой 8 или 3, что невозможно.

12. Любое целое число можно представить в одном из следующих видов: $9k$; $9k \pm 1$; $9k \pm 2$; $9k \pm 3$; $9k \pm 4$.

Их квадраты будут:

$(9k)^2 = 9(9k^2)$;
$(9k \pm 1)^2 = 9(9k^2 \pm 2k) + 1$;
$(9k \pm 2)^2 = 9(9k^2 \pm 4k) + 4$;
$(9k \pm 3)^2 = 9(9k^2 \pm 6k + 1)$;
$(9k \pm 4)^2 = 9(9k^2 \pm 8k + 1) + 7$.

Отсюда видим, что квадрат целого числа при делении на 9 может иметь только один из четырех остатков: 0, 1, 4, 7.

13. $S_n = 7(1 + 11 + 111 + \ldots + \underbrace{111\ldots1}_{n \text{ цифр}}) = 7\left(\dfrac{10-1}{9} + \dfrac{10^2-1}{9} + \dfrac{10^3-1}{9} + \ldots + \dfrac{10^n-1}{9}\right) = \dfrac{7}{81}(10^{n+1} - 9n - 10)$.

14. Рассмотрим число:

$$(2^{2^n}+1)+3=2^2(2^{2^n-2}+1)=2^2\,(4^{\,2^{n-1}-1}+1).$$

Показатель $2^{n-1}-1$ — число нечетное, значит, $4^{\,2^{n-1}-1}+1$ делится на $4+1$ и поэтому $(2^{2^n}+1)+3=2^2(4+1)m=10p$, откуда $2^{2^n}+1=10p-3$. В правой части имеем число, оканчивающееся цифрой 7.

15. $\underbrace{444\ldots4}_{n\text{ цифр}}\underbrace{888\ldots8}_{n\text{ цифр}}=4\cdot\dfrac{10^n-1}{9}\cdot10^n+8\cdot\dfrac{10^n-1}{9}=$

$$=\left[\frac{2}{3}(10^n-1)\right]\cdot\left[\frac{2}{3}(10^n-1+3)\right]=\underbrace{(666\ldots6}_{n\text{ цифр}})\cdot\underbrace{(666\ldots68}_{n\text{ цифр}}).$$

16. $\underbrace{111\ldots1}_{n\text{ цифр}}\underbrace{555\ldots56}_{n\text{ цифр}}=\dfrac{10^{n+1}-1}{9}\cdot10^{n+1}+5\cdot10\cdot\dfrac{10^n-1}{9}+6=$

$$=\left(\frac{10^{n+1}+2}{3}\right)^2=\left(\frac{10^{n+1}-1}{3}+1\right)^2=(\underbrace{333\ldots3}_{n\text{ цифр}}+1)^2.$$

17. $mn(m^4-n^4)=n(m^5-m)-m(n^5-n)$ кратно 30 (см. задачу 5).

18. Уравнение $y^2=3x^2+2$ неразрешимо в целых числах. В самом деле, число y либо можно написать как $y=3n$, либо $y=3n\pm1$; отсюда видим, что y^2 при делении на 3 дает в остатке 0 или 1, но не 2, как этого требует правая часть уравнения.

19. $N^2=1000(x+1)+100x+10(x+2)+(x+3)=11(101x+93)$. Отсюда $N=11k$ и потому $11k^2=101x+93$, $k^2=9x+8+\dfrac{2x+5}{11}$. Легко видеть, что $x=3$. Искомое число $4356=66^2$.

20. Имеем: $7^2x+7y+z=9^2z+9y+x$. Отсюда $y=8(3x-5z)$. Так как система семиричная, то $y<7$ и, следовательно, $3x-5z=0$. Поэтому $\dfrac{x}{5}=\dfrac{z}{3}$, отсюда $x=5$, $y=0$, $z=3$. Искомое число $503_{(7)}$.

21. Умножив и разделив $(n+1)(n+2)\ldots(n+n)$ на $n!$, получим $\dfrac{[1\cdot2\cdot3\cdot\ldots\cdot n(n+1)(n+2)\ldots(n+n)}{1\cdot2\cdot3\cdot\ldots\cdot n}=\dfrac{(2n)!}{n!}$; в составе $(2n)!$ содержится n четных и n нечетных сомножителей:

$$\frac{(2n)!}{n!}=\frac{[1\cdot3\cdot5\cdot\ldots\cdot(2n-1)]\cdot(2\cdot4\cdot6\ldots2n)}{n!}=$$

$$=\frac{[1\cdot3\cdot5\cdot\ldots\cdot(2n-1)]\,(1\cdot2\cdot3\cdot\ldots\cdot n)\,2^n}{n!}=1\cdot3\cdot5\cdot\ldots\cdot(2n-1)\cdot2^n,$$

откуда и следует, что $(n+1)(n+2)\ldots(n+n)=1\cdot3\cdot5\cdot\ldots\cdot(2n-1)\,2^n$ делится на 2^n.

22. 1) 21. 2) 13. 4) 119.

23. 1) 2520. 2) 138 600. 3) 99 671.

24. Пусть $(a, b, c) = d$, тогда из равенств

$$a = cq + r,\ b = cq_1 + r_1 \tag{1}$$

следует:

$$d/r \text{ и } d/r_1.$$

Покажем теперь, что $d = (c, r, r_1)$. Допустим, что $(c, r, r_1) = D$; тогда, обращаясь к равенствам (1), видим, что D/a, D/b и по допущению D/c, следовательно, $D = (a, b, c)$, а это значит $D = d$.

Для n чисел будем иметь $(a_1, a_2, \ldots, a_n) = (a_n, r_1, r_2, \ldots, r_{n-1})$, где $r_1, r_2, \ldots, r_{n-1}$ — остатки от деления $a_1, a_2, \ldots, a_{n-1}$ на a_n.

25. 1) 23. 2) 7. 3) 21.

26. 1) 3276. 2) 1116. 3) 67 818.

27. Если $(a,b) = 24$, то $a = 24m$ и $b = 24n$, где $(m, n) = 1$. Пусть для определенности $m < n$. Пользуясь равенством $[a, b] = \dfrac{ab}{(a, b)}$, имеем $2496 = \dfrac{24m \cdot 24n}{24}$, откуда $mn = 104 = 2^3 \cdot 13$.

Так как $(m, n) = 1$, то $mn = 1 \cdot 104$ или $mn = 8 \cdot 13$.

Теперь получаем:

при $m = 1$ и $n = 104$ будет $a = 24 \cdot 1 = 24$, $b = 24 \cdot 104 = 2496$;

при $m = 8$ и $n = 13$ будет $a = 24 \cdot 8 = 192, b = 24 \cdot 13 = 312$.

28. Пусть x и y — искомые числа и $(x, y) = d$, тогда $x = dm$ и $y = dn$, где $(m, n) = 1$. Теперь в силу условия

$$x + y = d(m + n) = 667 = 23 \cdot 29. \tag{1}$$

По условию, $\dfrac{[x\,y]}{(x, y)} = 120$, откуда

$$[x, y] = 120 \cdot (x, y) = 120d. \tag{2}$$

С другой стороны, по известной формуле имеем:

$$[x, y] = \frac{xy}{d}. \tag{3}$$

Из (2) и (3) следует $\dfrac{xy}{d} = 120d$, или $xy = 120\,d^2$.

Таким образом, получаем систему:

$$\begin{cases} x + y = 23 \cdot 29, \\ xy = 120\,d^2. \end{cases}$$

По (1) $d(m + n) = 23 \cdot 29$, откуда следует, что $d = 23$ и $d = 29$ ($d = 1$ или $d = 23 \cdot 29$ — непригодно, что легко усматривается). При $d = 23$ получаем $x = 552$, $y = 115$, при $d = 29$ получаем $x = 435$, $y = 232$.

29. Пусть x и y — искомые числа и $(x, y) = d$; тогда

$$\frac{x}{d} = m \text{ и } \frac{y}{d} = n, \text{ где } (m, n) = 1.$$

По условию:

$$m + n = 18,$$

$$[x, y] = \frac{xy}{d} = \frac{dm \cdot dn}{d} = mnd = 975 = 3 \cdot 5^2 \cdot 13. \qquad (2)$$

Из (1) и (2) имеем:

$$m + n = 18,$$
$$mnd = 3 \cdot 5^2 \cdot 13,$$

откуда $m = 5$, $n = 13$, $d = 15$ и, следовательно,

$$x = 75 \text{ и } y = 195.$$

30. По условию, $a = 899$, $b = 493$. Пользуясь алгорифмом Евклида, имеем:

$$a = b \cdot 1 + 406;$$
$$b = 406 \cdot 1 + 87;$$
$$406 = 87 \cdot 4 + 58;$$
$$87 = 58 \cdot 1 + 29;$$
$$58 = 29 \cdot 2.$$

Рассматривая эти равенства, начиная с предпоследнего, получаем:

$$29 = 87 - 58 = 87 - (406 - 87 \cdot 4) = 87 \cdot 5 - 406 =$$
$$= (b - 406) \cdot 5 - 406 = 5b - 406 \cdot 6 = 5b - (a - b)\,6 =$$
$$= a\,(-6) + b \cdot 11.$$

Итак, $29 = 899x + 493y$, где $x = -6$ и $y = 11$.

31. 1) $17 = a \cdot (-10) + b \cdot 23 = ax + by$.

2) $43 = a \cdot (-4) + b \cdot 5 = ax + by$.

3) $47 = a \cdot 2 + b \cdot (-5) = ax + by$.

32. Пусть $(a, b, c) = d$, тогда $a = md$, $b = nd$, $c = kd$;

$$\frac{a+b}{2} = \frac{m+n}{2}d, \quad \frac{a+c}{2} = \frac{m+k}{2}d, \quad \frac{b+c}{2} = \frac{n+k}{2}d.$$

Отсюда видно, что d есть общий делитель чисел

$$\frac{a+b}{2}, \quad \frac{a+c}{2}, \quad \frac{b+c}{2}.$$

Докажем, что d будет и наибольшим делителем. Допустим, что $\left(\frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}\right) = D$, тогда

$$d/D, \qquad (1)$$

$$\frac{a+b}{2} = m_1 D, \qquad (2)$$

$$\frac{a+c}{2} = n_1 D, \tag{3}$$

$$\frac{b+c}{2} = k_1 D. \tag{4}$$

Складывая (2) и (3) и вычитая (4), находим:

$$a = (m_1 + n_1 - k_1) D.$$

Аналогично:

$$b = (m_1 - n_1 + k_1) D,$$
$$c = (-m_1 + n_1 + k_1) D.$$

Теперь видим, что a, b, c делятся на D и, следовательно,

$$D/d. \tag{5}$$

Сопоставляя (1) и (5), приходим к тому, что $D = d$, т. е. $(a, b, c) = \left(\frac{a+b}{2}, \frac{a+c}{2}, \frac{b+c}{2}\right)$.

33. 1) Положим $(a, b, c) = d$, тогда

$$(a, b) = md, \tag{1}$$
$$(a, c) = nd, \tag{2}$$
$$(b, c) = kd, \tag{3}$$

где $(m, n, k) = 1$. Из (1) и (2) следует, что a делится на dm и a делится на dn, следовательно, $a = dmn\alpha$. Такими же рассуждениями устанавливаем, что

$$b = d\,m\,k\,\beta,$$
$$c = d\,n\,k\,\gamma.$$

Здесь $(\alpha, \beta, \gamma) = 1$. Теперь находим:

$$[a, b, c] = d\,mnk\,\alpha\beta\gamma = \frac{d^4 m^2 n^2 k^2 \alpha\beta\gamma}{d^3 mnk} =$$
$$= \frac{(bmn\alpha)(d\,mk\beta)(dnk\gamma)\,d}{dm \cdot dn \cdot dk} = \frac{abc\,(a, b, c)}{(a, b)(a, c)(b, c)}.$$

2) Указание. Для доказательства воспользоваться формулой:

$$[a, b] = \frac{ab}{(a, b)}.$$

34. Пусть $(a, b) = d$, тогда $a = md$, $b = nd$, $(m, n) = 1$. Находим:

$$5a + 3b = (5m + 3n)\,d,$$
$$13a + 8b = (13m + 8n)\,d.$$

Получили, что $5a + 3b$ и $13a + 8b$ имеют общий делитель d.

Докажем, что он будет и наибольшим.
Допустим, что $(5a + 3b,\ 13a + 8b) = D$, тогда

$$\begin{aligned} &D \mid d, \\ &5a + 3b = m_1 D, \\ &13a + 8b = n_1 D. \end{aligned} \tag{1}$$

Отсюда находим:

$$\begin{aligned} a &= (8m_1 - 3n_1) D, \\ b &= (5n_1 - 13m_1) D. \end{aligned}$$

Видим, что D есть делитель чисел a и b и, значит,

$$D \mid d \tag{12}$$

Из условий (1) и (2) следует, что $d = D$.

35. $\dfrac{1}{a} + \dfrac{1}{a+b} = \dfrac{2a+b}{a(a+b)}$.

Так как $(a, b) = 1$, то и $(a, 2a + b) = 1$. Покажем, что $(2a + b, a + b) = 1$. Допустим, что $(2a + b, a + b) = d > 1$, тогда $2a + b = dm$, $a + b = dn$, $(m, n) = 1$; и, следовательно, $a = d(m - n)$, $b = d(2n - m)$, т. е. $d \mid a$ и $d \mid b$, что исключено условием задачи.

§ 3. Простые и составные числа

36. Для упрощения можно не выписывать из натурального ряда от 2321 до 2349 все четные числа и числа, оканчивающиеся нулем и цифрой 5, все они не будут простыми. Имеем: 2321, 2323, 2327, 2329, 2331, 2333, 2337, 2339, 2341, 2343, 2347, 2349.

Теперь исключаем из этих чисел числа, кратные 3; по признаку делимости на 3 находим, что числа 2331, 2337, 2343, 2349 кратны 3; после вычеркивания их остаются числа 2321, 2323, 2327, 2329, 2333, 2339, 2341, 2347. Дальше нужно вычеркнуть числа, кратные 7, так как чисел, кратных 5, уже нет. Сначала находим первое число, кратное 7, так: делим первое из оставшихся чисел на 7, получаем $2321 = 7 \cdot 331 + 4$; судя по остатку (не достает 3 до 7), первым числом, кратным 7, будет третье от взятого в натуральном ряду, т. е. число 2324; затем каждое седьмое из последующих: 2331, 2338, 2345, но все они уже вычеркнуты. Чисел, кратных 11, только одно — 2321, которое и вычеркиваем (следующие за ним, каждое одиннадцатое, числа 2332, 2343 уже вычеркнуты). Дальше находим первое число, кратное 13: делим первое из оставшихся чисел 2323 на 13, получаем $2323 = 13 \cdot 178 + 9$; опять, судя по остатку, первым числом, кратным 13, будет четвертое от взятого в натуральном ряду, т. е. число 2327, которое и вычеркиваем; следующее тринадцатое число 2340 уже вычеркнуто. Так как $\sqrt{2350} < 49$, то дальше продолжаем вычеркивать числа, кратные последующим простым числам до 47 включительно; вычеркнутся числа: 2329 — кратное 17 и 2323 — кратное 23. Оставшиеся числа 2333, 2339, 2341, 2347 и являются простыми.

37. Числа 2647, 2657, 2659, 2663, 2671, 2677.

39. $2^{18} + 3^{18} = (2^2 + 3^2)(2^4 - 2^2 \cdot 3^2 + 3^4)(2^{12} - 2^6 \cdot 3^6 + 3^{12}) = 13 \cdot 61(2^{12} - 2^6 \cdot 3^6 + 3^{12}) = 13 \cdot 61 \cdot 488\,881 = 13 \times 61 \cdot 37 \cdot 73 \cdot 181$.

40. $n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2n + 2)(n^2 - 2n + 2)$.

41. Все натуральные числа можно представить так: $5n$, $5n \pm 1$, $5n \pm 2$. Числа вида $5n$ являются простыми только при $n = 1$; в этом случае $p = 5$, $4p^2 + 1 = 101$, $6p^2 + 1 = 151$, т. е. мы нашли одно значение p, удовлетворяющее условию.

Покажем теперь, что других значений p нет. Если $p = 5n \pm 1$, то $4p^2 + 1 = 5(20n^2 \pm 8n + 1)$ — число составное; если $p = 5n \pm 2$, то $6p^2 + 1 = 5(30n^2 \pm 24n + 1)$ — число составное.

42. Все натуральные числа можно представить так: $6k$, $6k \pm 1$, $6k \pm 2$, $6k + 3$. Простыми числами, кроме 2 и 3, могут быть только числа вида $6k \pm 1$. (Заметим, кстати, что обратное утверждение не всегда имеет место: не всякое число вида $6k \pm 1$— простое). Если взять $p = 6k - 1$, то тогда $p + 10 = 6k - 1 + 10 = 3(2k + 3)$ — число составное; если взять $p = 6k + 1$, то тогда $p + 14 = 6k + 1 + 14 = 3(2k + 5)$ — число составное. Таким образом, мы доказали, что не существует простого числа $p > 3$ такого, чтобы одновременно $p + 10$ и $p + 14$ тоже были простыми.

Возьмем $p = 2$, тогда $p + 10$ и $p + 14$ — составные; если же возьмем $p = 3$, тогда $p + 10$ и $p + 14$ — простые.

Итак, мы нашли только одно значение $p = 3$, удовлетворяющее условию.

43. Допустим противное, что при некотором k число $p = 6k - 1$ — последнее простое число. Возьмем число $N = 2 \cdot 3 \cdot 5 \cdot 7 \times 11 \ldots (p - 1)$. Первое слагаемое в правой части имеет множитель $2 \cdot 3 = 6$, поэтому можно записать $N = 6l - 1$. Все простые делители этого числа имеют вид $6m \pm 1$. Так как произведение чисел вида $6m + 1$ имеет тот же вид, в чем легко убедиться, то число N имеет еще простой делитель вида $q = 6t - 1$. С другой стороны, число N не делится ни на одно из простых чисел 2, 3, ..., p, поэтому $q > p$, что противоречит допущению.

44. По условию, $a > 3$, $m = 3t + 1$, $n = 3t_1 + 2$. Простые числа, кроме 2 и 3, можно представить в виде $p = 6k \pm 1$ (см. задачу 42). Если $a = p = 6k + 1$, то тогда $a + n = 6k + 1 + 3t + 2 = 3(2k + t + 1)$ — число составное; если же $a = p = 6k - 1$, то $a + m = 6k - 1 + 3t + 1 = 3(2k + t)$ тоже число составное.

45. По условию, $2p + 1$ — точный куб, это значит, что $2p + 1 = (2x + 1)^3 = 8x^3 + 12x^2 + 6x + 1 = 2x(4x^2 + 6x + 3) + 1$, откуда $p = x(4x^2 + 6x + 3)$. Так как p — простое, то $x = 1$ и $p = 13$, поэтому $2p + 1 = 27 = 3^3$ — единственное.

46. Сначала покажем, что, начиная с 5, в натуральном ряду нет трех последовательных нечетных чисел, являющихся простыми.

Если $k = 2$, k, $k + 2$ — нечетные числа, то одно из них кратно 3. Действительно, пусть k не делится на 3, тогда оно имеет вид $k = 3n \pm 1$, но в таком случае либо $k - 2$, либо $k + 2$ кратно 3.

Теперь допустим, что простые числа располагаются парами с промежутками между ними в одно четное составное число (числа-близнецы) — такое расположение простых чисел является наиболее плотным; в этом случае их можно представить как $6n - 1$ и $6n + 1$, и их номера будут $2n - 1$ и $2n$. Действительно, полагая $n =$

$= 1, 2, 3, 4, 5, 6, \ldots$, получим числа $6n - 1 = 5, 11, 17, 23, 29, 35, \ldots$ (их номера $2n - 1 = 1, 3, 5, 7, 9, 11, \ldots$) и числа $6n + 1 = 7, 13, 19, 25, 31, 37, \ldots$ (их номера $2n = 2, 4, 6, 8, 10, 12, \ldots$).

Как видим, в обоих случаях каждое число больше своего утроенного номера:

$$6n - 1 > 3\,(2n - 1) \quad \text{и} \quad 6n + 1 > 3 \cdot 2n.$$

47. Представим числа натурального ряда так:

$$30k,\ 30k \pm 1,\ 30k \pm 2, \ldots,\ 30k \pm 15.$$

Из них простыми могут быть только числа

$$p = 30k \pm 1,\ 30k \pm 7,\ 30k \pm 11,\ 30k \pm 13.$$

Дальнейшее решение ясно.

48. Если между числами $p - 1$ и $p + 1$ поместить число $p > 3$, то полученное произведение $(p - 1)\ p(p + 1)$ из трех последовательных чисел делится на 3, но, по условию, p не делится на 3, значит, $(p - 1)\ (p + 1)$ делится на 3.

В то же время $(p - 1)\ (p + 1)$ делится на 8, так как $p - 1$ и $p + 1$ — два последовательных четных числа, из которых, если одно делится только на 2, то другое будет делиться по меньшей мере на 4.

Но $p^2 - q^2 = (p - 1)\ (p + 1) - (q - 1)\ (q + 1)$, причем $(p - 1)\ (p + 1)$ и $(q - 1)\ (q + 1)$ каждое делится на 3 и на 8, следовательно, $p^2 - q^2$ делится на 24.

49. Положим, что некоторое нечетное число $p = 2k + 1$ разлагается на множители $p = mn\ (m > n)$. Тогда найдутся такие x и y, что будет иметь место система:

$$\begin{cases} x + y = m, \\ x - y = n, \end{cases}$$

из которой

$$x = \frac{m + n}{2} \quad \text{и} \quad y = \frac{m - n}{2};$$

следовательно, при составном p будет:

$$p = mn = (x + y)\,(x - y) = x^2 - y^2 = \left(\frac{m + n}{2}\right)^2 - \left(\frac{m - n}{2}\right)^2.$$

Если p будет простое, то его можно единственным образом представить в виде произведения $p = (2k + 1) \cdot 1$. В этом случае $m = 2k + 1 = p$ и $n = 1$, следовательно,

$$p = \left(\frac{m + n}{2}\right)^2 - \left(\frac{m - n}{2}\right)^2 = \left(\frac{p + 1}{2}\right)^2 - \left(\frac{p - 1}{2}\right)^2.$$

Итак, если представление

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

является единственным, то p — простое, если же

$$p = \left(\frac{m + n}{2}\right)^2 - \left(\frac{m - n}{2}\right)^2,$$

то p — составное.

Замечание. Из решения задачи вытекает способ разложения нечетных чисел на множители $(x+y)(x-y)$: из равенства $p=x^2-y^2$ следует $p+y^2=x^2$, т. е. чтобы найти x и y, достаточно к числу p подобрать квадрат такого натурального числа $y\left(y\leqslant\frac{p-1}{2}\right)$, чтобы сумма $p+y^2$ была полным квадратом (x^2). Отыскав таким образом y и x, будем иметь:

$$p=(x+y)(x-y)=mn.$$

При испытаниях удобно пользоваться таблицей квадратов натуральных чисел и конторскими счетами.

50. 1) По таблице квадратов чисел отыскиваем ближайший к числу 6643 квадрат: $6724=82^2$, находим разность: $6724-6643=81=9^2$, таким образом, $6643+81=6724$, или $6643+9^2=82^2$; следовательно, $6643=82^2-9^2=(82+9)(82-9)=91\cdot 73=7\cdot 13\cdot 73$.

2) По таблице отыскиваем ближайший к числу 1769 квадрат — 1849, находим разность $1849-1769=80$ — не является квадратом: берем следующий квадрат 1936, разность $1936-1769=167$ не является квадратом; следующий квадрат $2025=45^2$, разность $2025-1769=256=16^2$ $(=y^2)$. Итак, $1769+16^2=45^2$; следовательно, $1769=(45+16)(45-16)=61\cdot 29$.

Замечание. Процесс является утомительным только тогда, когда приходится прибегать к многократным испытаниям для отыскания y^2.

3) $3551=67\cdot 53$.

4) $6497=89\cdot 73$.

51. Имеем: $N=a^2+b^2=c^2+d^2$. Числа a и b, c и d — разной четности. Пусть a и c, b и d — одинаковой четности. Далее имеем:

$$(a-c)(a+c)=(d-b)(d+b),$$

$$\frac{a-c}{d-b}=\frac{d+b}{a+c}=\frac{u}{v}.$$

Здесь члены первой дроби сократили на t, а второй на s:

$$a-c=tu, \qquad d+b=su,$$
$$a+c=sv, \qquad d-b=tv,$$

Отсюда

$$a=\frac{tu+sv}{2}; \qquad b=\frac{su-tv}{2}.$$

Теперь

$$N=a^2+b^2=\frac{1}{4}[(tu+sv)^2+(su-tv)^2]=\frac{1}{4}(u^2+v^2)(t^2+s^2).$$

52. $972^2+235^2=1\,000\,009=1000^2+3^2=293\cdot 3413$.

53. Рассмотрим разложение:

$$a^{10}+a^5+1=\frac{a^{15}-1}{a^5-1}=\frac{(a^3-1)(a^{12}+a^9+a^6+a^3+1)}{(a-1)(a^4+a^3+a^2+a+1)}=$$
$$=(a^2+a+1)(a^8-a^7+a^5-a^4+a^3-a+1);$$

здесь $a^{12}+a^9+a^6+a^3+1$ разделили обычным способом на a^4+a^3+a+1.

В таком случае:

$$3^{10}+3^5+1=(3^2+3+1)(3^8-3^7+3^5-3^4+3^3-3+1)=13\cdot 4561.$$

54. Если k — нечетное, то $1+2^k$ кратно $1+2=3$. Если k — четное число, то оно может быть только либо $k=2^n$, либо $k=2^n m$, где $m>1$ — нечетное число, либо $k=0$. Но $1+2^k=1+2^{2^n m}=1+(2^{2^n})^m$ кратно $1+2^{2^n}$ (при $k=0$ кратно 2). Итак, при всех k, кроме $k=2^n$, число $1+2^{2^n}$ есть составное.

55. Покажем, что для всех α и β, не подчиненных требованию $(\alpha,\beta)=1$, $(\alpha,\beta)=2^n$, число $a^\alpha+b^\beta$ есть составное. Действительно, если $(\alpha,\beta)=d>1$ — нечетное число, то

$$\alpha=dm,\ \beta=dk,\ (m,k)=1$$

и $a^\alpha+b^\beta=(a^m)^d+(b^k)^d$ кратно a^m+b^k. Если же $(\alpha,\beta)=2^n d$ есть число четное, причем $d>1$ — нечетное, то

$$\alpha=2^n dm,\ \beta=2^n dk,$$

$$a^\alpha+b^\beta=(a^{2^n m})^d+(b^{2^n k})^d \text{ кратно } a^{2^n m}+b^{2^n k}.$$

Итак, при любых α и β, кроме $(\alpha,\beta)=1$ и $(\alpha,\beta)=2^n$, число $a^\alpha+b^\beta$ — составное.

Обратное утверждение неверно. Например, число $2^4+3^2=25$ — составное.

56. Допустим, что n — составное, $n=ab$ $(a>1,\ b>1)$, тогда $2^n-1=2^{ab}-1=(2^a)^b-1$ — число составное.

Обратное утверждение неверно: 2^p-1 не всегда простое. Например, $2^{11}-1=23\cdot 89$; $2^{23}-1=47\cdot 178\,421$.

ГЛАВА II

ЧИСЛОВЫЕ ФУНКЦИИ

§ 4. Функция $\pi(x)$

57. 1) 2; 2) 4; 3) 4; 4) 5; 5) 9; 7) 15; 9) 46; 11) 95;

58. 1) $\ln 50=3{,}9120\approx 3{,}91$; $\pi(x)\approx\dfrac{50}{3{,}91}\approx 13$;

$$\omega=\frac{\Delta\pi(x)}{\pi(x)}=\frac{15-13}{15}=\frac{2}{15}\approx 0{,}13=13\%.$$

2) ≈ 22, $\omega=12\%$; 3) ≈ 80, $\omega=16\%$; 4) ≈ 145, $\omega=14\%$.

§ 5. Функция $[x]$

59. 1) $2<\dfrac{8}{3}<3$, следовательно, $\left[\dfrac{8}{3}\right]=2$;2)0;

3) 2; 4) 0; 5) $-4 < -3\frac{1}{2} < -3$, следовательно, $\left[-3\frac{1}{2}\right] = -4$; 6) -3; 8) 5; 10) 3; 12) $4 < \sqrt[4]{580} < 5$ и $5 < \sqrt[4]{580} + 1 < 6$, следовательно, $[\sqrt[4]{580} + 1] = 5$; 14) $0 < \cos\frac{101\pi}{204} < 1$ и $4 < 4 + \cos\frac{101\pi}{204} < 5$, следовательно, $\left[4 + \cos\frac{101\pi}{204}\right] = 4$; 16) 1; 18) $-4 < -\lg 2512 < -3$ и $-2 < 2 - \lg 2512 < -1$, следовательно, $[2 - \lg 2512] = -2$; 20) -3.

60. Пусть $x = [x] + \theta_1$ и $y = [y] + \theta_2$, где $0 \leqslant \theta_1 < 1$ и $0 \leqslant \theta_2 < 1$, тогда $x + y = [x] + [y] + (\theta_1 + \theta_2)$. Если $0 \leqslant \theta_1 + \theta_2 < 1$, то $[x + y] = [x] + [y]$; если же $1 \leqslant \theta_1 + \theta_2 < 2$, то $[x + y] > [x] + [y]$. Объединяя результаты, получаем: $[x + y] \geqslant [x] + [y]$.

61. Из условия по определению функции $[x]$ имеем:

$$ax = m + \theta, \text{ где } 0 \leqslant \theta < 1 \text{ и } a \neq 0,$$

отсюда

$$x = \frac{m + \theta}{a}.$$

62. Из условия по определению функции $[x]$ имеем:

$$12{,}4m = 86 + \theta, \text{ где } 0 \leqslant \theta < 1.$$

Умножаем члены равенства на 5:

$$62m = 430 + 5\theta,$$

откуда $m = \frac{430 + 5\theta}{62} = 6 + \frac{58 + 5\theta}{62}$. Так как $0 \leqslant \theta < 1$, то $0 \leqslant 5\theta < 5$. Чтобы получить целое положительное m, число $\frac{58 + 5\theta}{62} = t$ должно быть целым. Полагая $t = 1$, получаем $\theta = \frac{4}{5}$ и $m = 7$.

При других целых значениях t требование $0 \leqslant \theta < 1$ не соблюдается.

63. По условию, $0 \leqslant \theta < 1$, отсюда

$$\frac{1}{2} \leqslant \theta + \frac{1}{2} < 1\frac{1}{2}, \tag{1}$$

$$0 \leqslant 2\theta < 2; \tag{2}$$

Рассматривая неравенства (1) и (2), видим, что если $\left[\theta + \frac{1}{2}\right] = 0$, то и $[2\theta] = 0$, и тогда $\left[\theta\right] + \left[\theta + \frac{1}{2}\right] = \left[2\theta\right]$; если же $\left[\theta + \frac{1}{2}\right] = 1$, то и $[2\theta] = 1$ и опять $\left[\theta\right] + \left[\theta + \frac{1}{2}\right] = \left[2\theta\right]$.

64. Пусть время поездки в первый раз было x дней, тогда дневной путь по x *км* составит весь путь в x^2 *км*. Во второй раз путешественник потратил $x+37$ дней и в каждые два дня из трех проезжал по 40 *км*, из $x+37$ дней он отдыхал $\left[\frac{x+37}{3}\right]$ дней, следовательно, в движении он был $x+37-\left[\frac{x+37}{3}\right]$ дней. Получаем уравнение:

$$20\left(x+37-\left[\frac{x+37}{3}\right]\right)=x^2.$$

Пусть $\left[\frac{x+37}{3}\right]=\frac{x+37}{3}-\theta$, где $\theta=0$, $\frac{1}{3}$, $\frac{2}{3}$, так как $x+37$ — число целое. При $\theta=0$ и $\theta=\frac{2}{3}$ решений нет.

При $\theta=\frac{1}{3}$ получаем $20\left(x+37-\frac{x+37}{3}+\frac{1}{3}\right)=x^2$, или, после преобразований, $3x^2-40x-1500=0$, откуда $x=30$.

65. Наибольший показатель α, с каким простое число p входит множителем в $n!$, находится по формуле:

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

где $p^k\leqslant n<p^{k+1}$ (см. Л. Я. Окунев, *Краткий курс теории чисел*, 1956, стр. 87 или И. М. Виноградов, *Основы теории чисел*, ГИТТЛ, 1952, стр. 25). Применяя ее, имеем:

$$\alpha=\left[\frac{100}{3}\right]+\left[\frac{100}{3^2}\right]+\left[\frac{100}{3^3}\right]+\left[\frac{100}{3^4}\right]=33+11+3+1=48,$$

следовательно, 100! делится на 3^{48}.

Замечание. Так можно разложить $n!$ на простые множители, беря за p последовательно все простые числа, меньшие n.

66. $\alpha=98$.

67. Число 100! оканчивается столькими нулями, сколько раз число 5 в паре с числом 2 входит сомножителем в число 100!, поэтому имеем $\left[\frac{100}{5}\right]+\left[\frac{100}{5^2}\right]=20+4=24$ нуля.

68. 1) $\left[\frac{10}{2}\right]+\left[\frac{10}{2^2}\right]+\left[\frac{10}{2^3}\right]=5+2+1=8;$

$$\left[\frac{10}{3}\right]+\left[\frac{10}{3^2}\right]=3+1=4;\quad\left[\frac{10}{5}\right]=2;\quad\left[\frac{10}{7}\right]=1.$$

Следовательно, $10!=2^8\cdot3^4\cdot5^2\cdot7$.

2) $15!=2^{11}\cdot3^6\cdot5^3\cdot7^2\cdot11\cdot13$.

3) $20!=2^{18}\cdot3^8\cdot5^4\cdot7^2\ 11\cdot13\cdot17\cdot19$.

4) $25!=2^{22}\cdot3^{10}\cdot5^6\cdot7^3\cdot11^2\cdot13\cdot17\cdot19\cdot23$.

5) $30!=2^{26}\cdot3^{14}\cdot5^7\cdot7^4\cdot11^2\cdot13^2\cdot17\cdot19\cdot23\cdot29$.

69. Количество целых положительных чисел, не превосходящих n и взаимно простых с каждым из простых чисел $p_1, p_2, \ldots, p_k$, вычисляется по формуле:

$$B(n;\ p_1,\ p_2, \ldots,\ p_k) = [n] - \left[\frac{n}{p_1}\right] - \ldots - \left[\frac{n}{p_k}\right] + \left[\frac{n}{p_1 p_2}\right] + \ldots +$$
$$+ \left[\frac{n}{p_{k-1} p_k}\right] - \left[\frac{n}{p_1 p_2 p_3}\right] - \ldots - \left[\frac{n}{p_{k-2}\, p_{k-1}\, p_k}\right] + \ldots +$$
$$+ (-1)^k \left[\frac{n}{p_1 p_2 \ldots p_k}\right].$$

(См. Л. Я. Окунев, *Краткий курс теории чисел*, 1956, стр 89.)

При $n = 180$ и $p_1 = 5$, $p_2 = 7$, $p_3 = 11$ имеем:

$$B(180;\ 5,7,11) = [180] - \left[\frac{180}{5}\right] - \left[\frac{180}{7}\right] - \left[\frac{180}{11}\right] + \left[\frac{180}{5\cdot 7}\right] + \left[\frac{180}{5\cdot 11}\right] +$$
$$+ \left[\frac{180}{7\cdot 11}\right] - \left[\frac{180}{5\cdot 7\cdot 11}\right] = 180 - 36 - 25 - 16 + 5 + 3 + 2 - 0 = 113.$$

70. $B\ (2311;\ 5,\ 7,\ 13,\ 17) = 1378.$

71. $B\ (100;\ 2,3) = 33.$

72. $B\ (12\,317;\ 3,\ 5,\ 7) = 5634.$

73. Достаточно найти количество чисел, не превосходящих 1000 и взаимно простых с числом $363 = 3 \cdot 11^2$, а затем, вычтя это количество из всех чисел, не превосходящих 1000, мы получим количество чисел, не взаимно простых с числом 1000 и не превосходящих 1000.

Ответ: 393.

74. Не вычеркнутыми будут числа, взаимно простые с 5, 8, 9. Числа 5, 8, 9 попарно простые и являются делителями 1800, следовательно, невычеркнутых чисел будет $B(1800;\ 5,\ 8,\ 9)$. Вычисляя, получаем $B\ (1800;\ 5,\ 8,\ 9) = 1120$.

75. $B\ (x;\ 2,\ 3,\ \ldots,\ p)$ есть число чисел, меньших x и не делящихся на 2, 3,..., p, причем p есть ближайшее простое число к $[\sqrt{x}]$ и не превосходящее $\sqrt{x}$. Но такие числа будут простыми. Следовательно, $B(x;\ 2,\ 3,\ \ldots,\ p)$ есть число всех простых чисел, меньших x, включая 1 и исключая k чисел: 2, 3, ..., p:

$$\pi\ (x) = B\ (x;\ 2,\ 3,\ \ldots,\ p) + k - 1.$$

76. Если x делится на $p_1, p_2, \ldots, p_k$, то

$$B(x;\ p_1,\ p_2,\ \ldots,\ p_k) = x\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right).$$

Из этого равенства легко определить x.

77. Чисел, делящихся на 2, будет $\left[\frac{120}{2}\right] = 60$; из них не делящихся на 3 и 5 будет $B\ (60;\ 3,5) = 32$. Чисел, кратных 3, будет $\left[\frac{120}{3}\right] = 40$, и среди них не делящихся на 2 и 5 будет $B\ (40;\ 2,5) = 16$.

Чисел, кратных 5, будет $\left[\frac{120}{5}\right]=24$, и среди них не делящихся на 2 и 3 будет $B(24, 2, 3)=8$. Чисел, делящихся на одно и только одно какое-нибудь из чисел 2, 3, 5, будет $32+16+8=56$.

78. Чисел, кратных 14, среди чисел от 1 до 5 000 будет $\left[\frac{5\,000}{14}\right]=357$, кратных 21, будет $\left[\frac{5\,000}{21}\right]=238$, кратных 10, будет $\left[\frac{5\,000}{10}\right]=500$. Всего этих чисел $357+238+500=1\,095$. Но в это число дважды вошли числа, кратные одновременно 14 и 21, т. е. кратные $[14, 21]=42$, их будет $\left[\frac{5\,000}{42}\right]=119$. Чисел, кратных одновременно 14 и 10, т. е. кратных 70, будет $\left[\frac{5\,000}{70}\right]=71$. В это число 71 вошли и числа, кратные $[21, 10]=210$, и числа, кратные $[14, 21, 10]=210$. Всего чисел, кратных хотя бы одному из чисел 14, 21, 10, будет $1\,095-119-71=905$. Благоприятных случаев 905, а всего случаев 5 000. Искомая вероятность $\frac{905}{5\,000}=0{,}181$.

79. Умножим и разделим $1\cdot3\cdot5\cdot\ldots\cdot(2m+1)$ на $2\cdot4\cdot6\cdot\ldots\cdot2m$:

$$1\cdot3\cdot5\cdot\ldots(2m+1)=\frac{(2m+1)!}{m!\,2^m}.$$

Наибольший показатель α, с которым простое число p содержится в каноническом разложении $(2m+1)!$, есть

$$\alpha=\left[\frac{2m+1}{p}\right]+\left[\frac{2m+1}{p^2}\right]+\ldots.$$

Соответственно для числа $m!$ показатель

$$\beta=\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\ldots,$$

а для числа $1\cdot3\cdot5\cdot\ldots\cdot(2m+1)=\frac{(2m+1)!}{m!\,2^m}$ равен разности:

$$\alpha-\beta=\left[\frac{2m+1}{p}\right]-\left[\frac{m}{p}\right]+\left[\frac{2m+1}{p^2}\right]-\left[\frac{m}{p^2}\right]+\ldots$$

80. Обе части будут равны нулю при условии

$$0\leqslant\frac{x}{a}<\frac{x}{a-1}<1.$$

Отсюда

$$0\leqslant x<a-1.$$

Решения будут $x=0, 1, 2, \ldots, a-2$ ($a-1$ решений). Пусть теперь

$$\left[\frac{x}{a}\right]=\left[\frac{x}{a-1}\right]=1,$$

т. е.

$$1 \leqslant \frac{x}{a} < \frac{x}{a-1} < 2,$$

откуда

$$a \leqslant x < 2(a-1).$$

Решения: $x = a,\ a+1,\ a+2,\ \ldots,\ 2a-3$ ($a-2$ решений). Аналогично для случая

$$\left[\frac{x}{a}\right] = \left[\frac{x}{a-1}\right] = 2$$

находим: $x = 2a,\ 2a+1,\ 2a+2,\ \ldots,\ 3a-4$ ($a-3$ решений). Наконец, для

$$\left[\frac{x}{a}\right] = \left[\frac{x}{a-1}\right] = a-2$$

найдем:

$$a-2 \leqslant \frac{x}{a} < \frac{x}{a-1} < a-1,$$

$$a^2-2a \leqslant x < a^2-2a+1,\ x = a^2-2a \text{ (одно решение)}.$$

Если взять $\left[\frac{x}{a}\right] = \left[\frac{x}{a-1}\right] = a-1,\ a,\ a+1,\ \ldots,$ то решений не будем иметь.

Всего решений: $(a-1)+(a-2)+(a-3)+\ldots+2+1 = \frac{a(a-1)}{2} = C_a^2$.

81. Пусть $[x] = a$, тогда $x = a+\theta$, $0 \leqslant \theta < 1$.

Всегда можно указать такое r, что

$$\frac{r}{n} \leqslant \theta < \frac{r+1}{n}.$$

Напишем левую часть в виде:

$$[x] + \left[x+\frac{1}{n}\right] + \ldots + \left[x+\frac{n-r-1}{n}\right] + \left[x+\frac{n-r}{n}\right] + \ldots + \left[x+\frac{n-1}{n}\right].$$

Покажем, что каждое слагаемое от $[x]$ до $\left[x+\frac{n-r-1}{n}\right]$ равно a.

Действительно, самое наибольшее из них

$$x+\frac{n-r-1}{n} = a+\theta+\frac{n-r-1}{n} < a+\frac{r+1}{n}+\frac{n-r-1}{n} = a+1.$$

Следовательно,

$$\left[x+\frac{n-r-1}{n}\right] = a.$$

Этих слагаемых $n-r$, их сумма равна $a(n-r)$. Аналогично можно показать, что каждое слагаемое суммы

$$\left[x+\frac{n-r}{n}\right]+\left[x+\frac{n-r+1}{n}\right]+\ldots+\left[x+\frac{n-1}{n}\right]$$

равно $a+1$. Число этих слагаемых r, их сумма равна $r(a+1)$. Сумма всей левой части $a(n-r)+r(a+1)=na+r$. Правая часть $[nx]=[n(a+\Theta)]=[na+n\Theta]=na+r$, так как из неравенства

$$\frac{r}{n}\leqslant\Theta<\frac{r+1}{n}$$

следует

$$r\leqslant n\Theta<r+1.$$

§ 6. Функция $\{x\}$.

82. 1) $\{2,6\}=2,6-2=0,6$; 2) $\frac{2}{3}$; 3) 0; 4) $\{-4,35\}=-4,35-(-5)=0,65$; 6) $\frac{1}{2}$.

§ 7. Функции $\sigma(a)$ и $\tau(a)$

83. 1) Находим простые делители числа $375=3\cdot5^3$. Теперь по формулам имеем:

$$\sigma(375)=\frac{3^{1+1}-1}{3-1}\cdot\frac{5^{3+1}-1}{5-1}=\frac{8}{2}\cdot\frac{624}{4}=624,$$

$$\tau(375)=(1+1)\cdot(3+1)=2\cdot4=8.$$

2) 2418; 30. 3) 1440; 8. 4) 1960; 12.5) 2808; 24. 6) 3844; 30.

84. 1) Находим каноническое разложение числа: $360=2^3\times3^2\cdot5$. Теперь имеем: $(1+2+4+8)(1+3+9)\cdot(1+5)=1+2+4+8+3+6+12+24+9+18+36+72+5+10+20+40+15+30+60+120+45+90+180+360$ — все делители числа 360, записанные в виде слагаемых.

2) $1+5+25+125+3+15+75+375$.

85. Пусть $N=p^\alpha q^\beta$, где p и q—простые числа. По условию, $(\alpha+1)(\beta+1)=6$, отсюда $\alpha=1$, $\beta=2$; следовательно, $N=pq^2$. Далее, по условию, $(1+p)(1+q+q^2)=28$. Так как $1+q+q^2=1+q(1+q)$ — число нечетное, поскольку $q(q+1)$ — четное, то $1+q+q^2=7$ и $1+p=4$, откуда $q=2$ и $p=3$. Искомое число $N=p\cdot q^2=3\cdot2^2=12$.

86. Число $N=p^\alpha q^\beta$ имеет $(\alpha+1)(\beta+1)$ делителей,
число $N^2=p^{2\alpha}p^{2\beta}$ имеет $(2\alpha+1)(2\beta+1)$ делителей,
число $N^3=p^{3\alpha}q^{3\beta}$ имеет $(3\alpha+1)(3\beta+1)$ делителей.
По условию, $(2\alpha+1)(2\beta+1)=15$, откуда $\alpha=1$, $\beta=2$ (или $\alpha=2$, $\beta=1$) и, следовательно, $(3\alpha+1)(3\beta+1)=4\cdot7=28$.

87. Возвышая произведение $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha}$ в k-ю степень, будем иметь: $\left(p_1^{\alpha_1}\right)^k\left(p_2^{\alpha_2}\right)^k\ldots\left(p_n^{\alpha}\right)^k=\left(p_1^k\right)^{\alpha_1}\left(p_2^k\right)^{\alpha_2}\ldots\left(p_n^k\right)^{\alpha}$.

Искомая сумма всех делителей, каждый из которых взят в k-й степени, будет получена, если в формуле

$$\sigma(N) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_n^{\alpha_n+1}-1}{p_n-1}$$

заменим $p_1, p_2, \ldots, p_n$ через $p_1^k, p_2^k, \ldots, p_n^k$ и левую часть условно обозначим через $\sigma_k(N)$:

$$\sigma_k(N) = \frac{p_1^{k(\alpha_1+1)}-1}{p_1^k-1} \cdot \frac{p_2^{k(\alpha_2+1)}-1}{p_2^k-1} \cdot \ldots \cdot \frac{p_n^{k(\alpha_n+1)}-1}{p_n^k-1}.$$

88. 1) Каноническое разложение числа: $12 = 2^2 \cdot 3$. По формуле имеем:

$$\sigma_2(12) = \frac{2^{2(2+1)}-1}{2^2-1} \cdot \frac{3^{2(1+1)}-1}{3^2-1} = \frac{63}{3} \cdot \frac{80}{8} = 210.$$

2) 455. 4) 341.

89. Действительно,

$$\sigma(28) = \frac{2^3-1}{2-1} \cdot \frac{7^2-1}{7-1} = 7 \cdot \frac{48}{6} = 28 \cdot 2.$$

Аналогично поступаем и для чисел 496 и 8128.

90. Выпишем все делители числа N:

$$1, a_1, a_2, \ldots, \frac{N}{a_2}, \frac{N}{a_1}, \frac{N}{1}.$$

Каждому делителю a_i соответствует делитель $\frac{N}{a_i}$, следовательно, число делителей — четное, за исключением случая, когда $N = a^2$, т. е. когда делителю a соответствует тот же делитель $\frac{N}{a} = \frac{a^2}{a} = a$.

Перемножая каждую пару делителей, получаем $a_i \frac{N}{a_i} = N$, и таких пар будет $\frac{n}{2}$, где n — число делителей.

Таким образом, произведение всех делителей:

$$P = \left(a_i \frac{N}{a_i}\right)^{\frac{n}{2}} = N^{\frac{n}{2}}.$$

Эта формула включает и случай, когда $N = a^2$, ибо тогда

$$P = \left(a_i \frac{N}{a_i}\right)^{\frac{n-1}{2}} a = N^{\frac{n-1}{2}} \cdot N^{\frac{1}{2}} = N^{\frac{n}{2}}.$$

91. По условию, $P = 5832$, или $P = 2^3 \cdot 3^6$. Но произведение всех делителей числа вида $N = 2^\alpha \cdot 3^\beta$ будет:

$$P = (2^\alpha \cdot 3^\beta)^{\frac{(\alpha+1)(\beta+1)}{2}},$$

следовательно,

$$(2^\alpha \cdot 3^\beta)^{\frac{(\alpha+1)(\beta+1)}{2}} = 2^3 \cdot 3^6,$$

отсюда

$$\alpha(\alpha + 1)(\beta + 1) = 6, \quad \beta(\alpha + 1)(\beta + 1) = 12,$$

что дает

$$\alpha = 1, \ \beta = 2 \text{ и } N = 2 \cdot 3^2 = 18.$$

92. Возьмем $N = 3^\alpha \cdot 5^\beta$, произведение всех делителей его

$$(3^\alpha \cdot 5^\beta)^{\frac{(\alpha+1)(\beta+1)}{2}} = 3^{30} \cdot 5^{40},$$

отсюда

$$\alpha(\alpha + 1)(\beta + 1) = 60, \quad \beta(\alpha + 1)(\beta + 1) = 80,$$

что дает

$$\alpha = 3, \ \beta = 4 \text{ и } N = 3^3 \cdot 5^4.$$

93. Указание. Воспользоваться тем обстоятельством, что

$$d_1 = \frac{N}{d_n}, \ d_2 = \frac{N}{d_{n-1}}, \ \ldots.$$

94. Напишем в порядке возрастания все делители числа N:

$$1, \ d_1, \ d_2, \ldots, \ \frac{N}{d_2}, \ \frac{N}{d_1}, \ \frac{N}{1},$$

их будет:

$$(\alpha + 1)(\beta + 1) \ldots (\mu + 1).$$

Соединяя попарно

$$1 \cdot \frac{N}{1}, \quad d_1 \cdot \frac{N}{d_1}, \quad d_2 \cdot \frac{N}{d_2}, \ldots,$$

получим все различные разложения, число которых будет:

$$\frac{(\alpha + 1)(\beta + 1) \ldots (\mu + 1)}{2}$$

для случая, когда N — неточный квадрат, и

$$\frac{1 + (\alpha + 1)(\beta + 1) \ldots (\mu + 1)}{2}$$

для случая, когда N — точный квадрат.

Объединяя эти результаты, получаем, что число различных разложений равно

$$\left[\frac{1+(\alpha+1)(\beta+1)\ldots(\mu+1)}{2}\right].$$

95. Решение приводит к системе:

$$\begin{cases}(\alpha+1)(\gamma+1)=8,\\(\alpha+1)(\beta+1)=12,\\(\beta+1)(\gamma+1)=6.\end{cases}$$

Перемножая, после преобразований, находим $N=1400$.

96. $N=2\cdot3\cdot5^4$.

§ 8. Функция Эйлера

97. 1) Каноническое разложение числа: $375=3\cdot5^3$. Теперь по формуле имеем: $\varphi(375)=3\cdot5^3\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=3\cdot5^3\times\times\frac{2}{3}\cdot\frac{4}{5}=200$. 2) 192. 4) 432. 6) 320. 8) 400. 10) 1152.

98. 1) $\varphi(17)=17-1=16$. 2) 30. 4) 70.

99. 1) $\varphi(3^5)=3^4\cdot2=162$. 2) 500. 4) 272.

100. 1) 40. 2) $\varphi(5\cdot7\cdot13)=\varphi(5)\varphi(7)\varphi(13)=4\cdot6\cdot12=288$. 4) $\varphi(12\cdot7)=\varphi(2^2\cdot3\cdot7)=2\cdot2\cdot6=24$. 6) 480. 10) 388 800.

101. Чисел, взаимно простых с числом 120 и меньших его, будет $\varphi(120)=32$, это числа 1, 7, 11, 13, ..., 119. Все остальные $120-32=88$ чисел будут с числом $30=2\cdot3\cdot5$ иметь общие делители, большие единицы.

102. По условию, $a=3^\alpha\cdot5^\beta\cdot7^\gamma$. Функция Эйлера от этого числа будет $\varphi(a)=3^{\alpha-1}\cdot2\cdot5^{\beta-1}\cdot4\cdot7^{\gamma-1}\cdot6=2^4\cdot3^\alpha\cdot5^{\beta-1}\cdot7^{\gamma-1}$. По условию, $\varphi(a)=3600=2^4\cdot3^2\cdot5^2$, следовательно, $2^4\cdot3^\alpha\cdot5^{\beta-1}\cdot7^{\gamma-1}=2^4\cdot3^2\cdot5^2$, откуда $\alpha=2$, $\beta=3$, $\gamma=1$ и $a=3^2\cdot5^3\cdot7=7875$.

103. Из условия имеем: $\varphi(a)=\varphi(pq)=(p-1)(q-1)=120$ и $p-q=2$. Получаем систему:

$$\begin{cases}(p-1)(q-1)=120,\\p-q=2;\end{cases}$$

решая ее, находим $p=13$, $q=11$ и, следовательно, $a=pq=143$.

104. Из условия имеем: $\varphi(a)=\varphi(p^2q^2)=p(p-1)q(q-1)$ и $\varphi(a)=11\,424=2^5\cdot3\cdot7\cdot17$, следовательно, $p(p-1)q(q-1)=2^5\cdot3\cdot7\cdot17$, или $p(p-1)q(q-1)=17\cdot16\cdot7\cdot6$, откуда $p=17$, $q=7$ и $a=17^2\cdot7^2=14\,161$.

105. Из условия имеем: $\varphi(a)=p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\ldots p_n^{\alpha_n-1}(p_n-1)$ и $\varphi(a)=462\,000=2^4\cdot3\cdot5^3\cdot7\cdot11$; следовательно,

$$p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\ldots p_n^{\alpha_n-1}(p_n-1)=2^4\cdot3\cdot5^3\cdot7\cdot11.$$

Перегруппируем сомножители в правой части так, как того требует левая часть:

$$p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\ldots p_n^{\alpha_n-1}(p_n-1)=(11\cdot10)(7\cdot6)(5^2\cdot4),$$

отсюда $p_1 = 11$ и $\alpha_1 = 2$; $p_2 = 7$ и $\alpha_2 = 2$; $p_3 = 5$ и $\alpha_3 = 3$; $a = 11^2 7^2 5^3 = 741\,125$.

106. Предварительно докажем, что если $(a, m) = 1$, то $(a, m - a) = 1$. Действительно, допустим противное, что $(a, m - a) = d > 1$, тогда $a = dk$ и $m - a = dt$, откуда $m = d(t + k)$ и $(a, m) = d > 1$, что невозможно, так как противоречит условию $(a, m) = 1$.

Теперь выпишем в порядке возрастания числа, меньшие m и с ним взаимно простые:

$$1,\ a_1,\ a_2,\ldots,\ m - a_2,\quad m - a_1,\ m - 1;$$

всего их $\varphi(m)$. Каждому числу a_i соответствует число $m - a_i$; сумма каждой пары $a_i + (m - a_i) = m$, число таких пар $\frac{1}{2}\varphi(m)$ и, следовательно, сумма всех пар:

$$S = \frac{1}{2} m\varphi(m).$$

107. 1) Применяя формулу $S = \frac{1}{2} m\varphi(m)$, получаем:

$S = \frac{1}{2} \cdot 12 \cdot 4 = 24$. Действительно, $1 + 5 + 7 + 11 = 24$.

3) 54. 5) 37 500.

108. Так как $\varphi(7^x) = 7^{x-1} \cdot 6$, то $7^{x-1} \cdot 6 = 705\,894$, или $7^{x-1} = 117\,649 = 7^6$, откуда $x - 1 = 6$ и $x = 7$.

109. Так как числителями можно брать только числа, взаимно простые с b и меньшие b, то всего искомых дробей будет $\varphi(b)$.

110. 1) 4 дроби, именно: $\frac{1}{10}, \frac{3}{10}, \frac{7}{10}, \frac{9}{10}$. 3) 12 дробей.

111. На основании решения задачи 77 дробей со знаменателем 2 будет $\varphi(2)$, со знаменателем 3 будет $\varphi(3)$ и т. д. и со знаменателем $b = n$ будет $\varphi(n)$; следовательно, число всех искомых дробей выразится суммой $\varphi(2) + \varphi(3) + \ldots + \varphi(n)$.

112. 1) Число всех положительных правильных несократимых дробей со знаменателями от 2 до 5 равно:

$$\varphi(2) + \varphi(3) + \varphi(4) + \varphi(5) = 1 + 2 + 2 + 4 = 9.$$

Действительно, этими дробями будут:

$\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}$, всего 9 дробей.

2) 31. 3) 71.

113. По условию, $(300, x) = 20$ и все значения x меньше 300. После сокращения на 20 должно быть $(15, y) = 1$, где все значения y меньше 15 и взаимно просты с 15; количество их $\varphi(15) = 8$. Это числа: $y = 1, 2, 4, 7, 8, 11, 13, 14$; тогда $x = 20, 40, 80, 140, 160, 220, 260, 280$.

114. $\varphi(45) = 24$.

115. $\varphi(36) = 12$.

116. Указание. Четность $\varphi(m)$ следует из решения задачи 106.

117. 1) $a = 72 = 2^3 \cdot 3^2$. Находим все делители числа 72 : $(1 + 2 + 2^2 + 2^3)(1 + 3 + 3^2)$. Теперь, не раскрывая скобок, возьмем функцию Эйлера от всех делителей, принимая $\varphi(1) = 1$. Получим:

$$\sum_{d|a} \varphi(d) = [\varphi(1) + \varphi(2) + \varphi(2^2) + \varphi(2^3)]\,[\varphi(1) + \varphi(3) + \varphi(3^2)] =$$

$$= (1 + 1 + 2 + 4)(1 + 2 + 6) = 8 \cdot 9 = 72 = a.$$

119. Имеем:

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

и потому в силу условия:

$$p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_n^{\alpha_n - 1}(p_n - 1) = 12.$$

Отсюда видим, что p_i может быть простым числом 2, 3, 5, 7, 11, 13. Учитывая предыдущую задачу, находим:

$$x = 13,\ 21,\ 26,\ 28,\ 42,\ 36.$$

120. Если допустить, что $(x, 6) = 1$, то равенство $\varphi(2x) = \varphi(3x)$ переходит в невозможное равенство $1 = 2$.

Итак, $(x, 6) = d > 1$. Пусть $x = 2^\alpha y$, где $(y, 6) = 1$. Равенство $\varphi(2x) = \varphi(3x)$ принимает вид:

$$\varphi(2^{\alpha+1} y) = \varphi(2^\alpha \cdot 3y).$$

Таким образом, $x = 2^\alpha y$ удовлетворяет уравнению.

Другие значения $x = 3^\beta y$, $x = 2^\alpha 3^\beta y$, где $(y, 6) = 1$, непригодны.

121. Решение аналогично решению предыдущей задачи.

122. Если p_i — различные простые нечетные числа, то $p_i - 1$ — числа четные:

$$p_i - 1 = 2^{\alpha_i} n_i,$$

где n_i — числа нечетные. По условию,
$\varphi(m) = (p_1 - 1)(p_2 - 1) \dots (p_k - 1) = 2^{\alpha_1 + \alpha_2 + \dots + \alpha_k} n_1 n_2 \dots n_k = 2^\beta \cdot 3$.
Отсюда $\alpha_1 + \alpha_2 + \dots + \alpha_k = \beta$, $n_1 n_2 \dots n_k = 3$, т. е. среди чисел p_i только одно вида $2^{\alpha_i} \cdot 3 + 1$, а остальные имеют вид $2^{\alpha_i} + 1$.

Пример 1. $\varphi(m) = 24 = 4 \cdot 6 = 2 \cdot 12$.
В первом случае $m = 5 \cdot 7 = (2^2 + 1) \cdot (2 \cdot 3 + 1)$.
Во втором случае $m = 3 \cdot 13 = (2 + 1)(2^2 \cdot 3 + 1)$.

Пример 2. $\varphi(m) = 48 = 4 \cdot 12 = 2 \cdot 4 \cdot 6$.
В первом случае $m = 5 \cdot 13 (2^2 + 1)(2^2 \cdot 3 + 1)$.
Во втором случае $m = 3 \cdot 5 \cdot 7 = (2 + 1)(2^2 + 1)(2 \cdot 3 + 1)$.

123. 1) Если $\varphi(x) = \frac{1}{2} x$, то $2/x$ $\left(\frac{1}{2} x$ — число целое$\right)$, $x = 2^\alpha n$, где n — число нечетное.

Тогда

$$\varphi(2^\alpha n) = \frac{1}{2} 2^\alpha n,$$

или

$$2^{\alpha-1}\varphi(n) = 2^{\alpha-1} n.$$

Отсюда имеем $\varphi(n) = n$, что может быть только при $n = 1$. Итак, $x = 2^\alpha$ — решение данного уравнения.

2) Если $\varphi(x) = \frac{2}{3} x$, то $3 \nmid x$, $x = 3^\beta n$, где $(n, 3) = 1$.

Теперь

$$\varphi(3^\beta n) = \frac{2}{3} 3^\beta n,$$

или

$$3^{\beta-1} \cdot 2\varphi(n) = \frac{2}{3} \cdot 3^\beta n, \ \varphi(n) = n = 1,$$

$x = 3^\beta$ — решение данного уравнения.

3) $x = 2^\alpha 3^\beta$.

4) Решения нет.

ГЛАВА III

СРАВНЕНИЯ

§ 9. Понятия о сравнениях и свойства сравнений

124. Если n — число нечетное, тогда $n - 1$ и $n + 1$ — последовательные четные числа. Если одно из них кратно 2, то другое по меньшей мере кратно 4, поэтому:

$$(n - 1)(n + 1) = n^2 - 1 \equiv 0 \pmod 8,$$

или $n^2 \equiv 1 \pmod 8$.

125. По формуле разложения степени бинома имеем:

$$(a + b)^p = a^p + pa^{p-1}b + \frac{p(p-1)}{2} a^{p-2}b^2 + \ldots + pab^{p-1} + b^p.$$

В правой части все члены, кроме a^p и b^p, делятся на p. Действительно, $C_p^n = \frac{p(p-1)(p-2)\ldots(p-n+1)}{1 \cdot 2 \cdot 3 \cdot \ldots \cdot n}$ — число целое, но p — число простое и не сокращается ни с одним из сомножителей знаменателя, так как $p > n$. Обозначив частное от деления $(a + b)^p$ на p через q, получим: $(a + b)^p = pq + a^p + b^p$, откуда следует сравнение:

$$(a + b)^p \equiv a^p + b^p \pmod p.$$

126. По условию, $100\,a + 10\,b + c \equiv 0 \pmod{21}$. Умножив члены этого сравнения на 4, получим:

$$400\,a + 40\,b + 4c \equiv 0 \pmod{21}, \qquad (1)$$

но

$$400\,a \equiv a \pmod{21},$$
$$40\,b \equiv -2b \pmod{21},$$
$$4\,c \equiv 4c \pmod{21}$$ — очевидное сравнение.

Сложив эти сравнения, будем иметь:

$$400\,a + 40\,b + 4c \equiv a - 2b + 4a \pmod{21}.$$

Но левая часть в силу (1) сравнима с нулем, следовательно, и

$$a - 2b + 4c \equiv 0 \pmod{21}.$$

127. Умножая обе части сравнения на $3^4 = 81$, получим:

$$3^{n+4} = -81 \pmod{10}.$$

Теперь, исключая из правой части число -80, кратное модулю, получим искомое сравнение:

$$3^{n+4} \equiv -1 \pmod{10}.$$

128. Так как $11 \cdot 31 - 1 = 340 = 5 \cdot 68$ и так как $2^5 \equiv -1 \pmod{11}$, то, возвышая члены этого сравнения в 68-ю степень, получим:

$$(2^5)^{68} = 2^{340} = 2^{11\cdot 31-1} \equiv 1 \pmod{11}. \qquad (1)$$

Далее, так как $2^5 \equiv 1 \pmod{31}$, то

$$(2^5)^{68} = 2^{11\cdot 31-1} \equiv 1 \pmod{31}. \qquad (2)$$

Теперь из (1) и (2) по третьему особому свойству имеем: $2^{11\cdot 31-1} \equiv 1 \pmod{11\cdot 31}$; умножая члены этого сравнения на 2, получаем искомое сравнение:

$$2^{11\cdot 31} \equiv 2 \pmod{11\cdot 31}.$$

129. Так как

$$\left.\begin{aligned} 11 &\equiv -3,\\ 18 &\equiv -3,\\ 2322 &\equiv -2,\\ 13 &\equiv -1,\\ 19 &\equiv -2, \end{aligned}\right\} \pmod 7,$$

где числа -3, -2, -1 — абсолютно наименьшие по абсолютной величине числа, сравнимые с остатками, получающимися при делении данных чисел на 7, то, перемножая эти сравнения (3-е основное свойство), получаем:

$$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv -36 \pmod 7.$$

Исключая из правой части число -35, кратное модулю (следствие 2-е из 2-го основного свойства), имеем:

$$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv -1 \pmod 7.$$

З а м е ч а н и е. Решение данной задачи кратко запишется так:

$$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv (-3)\,(-3)\,(-2)\,(-1)\,(-2) = -36 \equiv -1 \pmod 7.$$

В дальнейшем в подобных случаях будем пользоваться решением в такой краткой записи.

130. Имеем:

$$3^{14} = (3^3)^4 \cdot 3^2 = 27^4 \cdot 3^2 \equiv (-2)^4 \cdot 3^2 = 144 \equiv -1 \pmod{29}.$$

131. Так как $1532^5 \equiv 2^5 = 32 \equiv 5 \pmod 9$, то, вычитая из этого сравнения очевидное сравнение $1 \equiv 1 \pmod 9$, получаем $1532^5 - 1 \equiv 4 \pmod 9$, откуда следует, что остаток от деления $1532^5 - 1$ на 9 равен 4.

132. Напишем k сравнений:

$$\left.\begin{array}{l} p-1 \equiv -1, \\ p-2 \equiv -2, \\ p-3 \equiv -3, \\ \ldots\ldots \\ p-k \equiv -k. \end{array}\right\} \pmod p$$

Перемножив их, получим:
$(p-1)(p-2)(p-3)\ldots(p-k) \equiv (-1)^k \cdot 1 \cdot 2 \cdot 3 \cdot \ldots \cdot k \pmod p$. Так как $1 \cdot 2 \cdot 3 \cdot \ldots \cdot k, p) = 1$, то, разделив члены сравнения на $1 \cdot 2 \cdot 3 \cdot \ldots \cdot k$, будем иметь: $C_{p-1}^k = (-1)^k \pmod p$.

133. При $n = 5$ имеем $2^{2^5} + 1 = 2^{32} + 1$; но $2^{32} = (2^8)^4 = (256^2)^2 = 65\,536^2 \equiv 154^2 = 23\,716 \equiv -1 \pmod{641}$, следовательно, $2^{32} + 1 \equiv 0 \pmod{641}$. Действительно, $2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$.

Другое решение. Представим число 641 так:

$$641 = 640 + 1 = 5 \cdot 2^7 + 1, \tag{1}$$

$$641 = 625 + 16 = 5^4 + 2^4. \tag{2}$$

Из (1) имеем сравнение:

$$5 \cdot 2^7 \equiv -1 \pmod{641},$$

или

$$5^4 \cdot 2^{28} \equiv 1 \pmod{641}. \tag{3}$$

Из (2) следует, что

$$2^4 \equiv -5^4 \pmod{641}. \tag{4}$$

Перемножая сравнения (3) и (4), получаем:

$$5^4 \cdot 2^{32} \equiv -5^4 \pmod{641},$$

откуда

$$2^{32} + 1 \equiv 0 \pmod{641}.$$

134. Предварительно покажем, что если $(a, m) = k$, то и $(b, m) = k$. Из сравнения $a \equiv b \pmod m$ следует $a = mt + b$, или $b = a - mt$, откуда видно, что если $(a, m) = k$, то $k \mid b$. Таким образом, если $(a, m) = 1$, то и $(b, m) = 1$.

Теперь, по условию, имеем:

$$ac \equiv bd \pmod m, \tag{1}$$

$$a \equiv b \pmod m. \tag{2}$$

Умножая сравнение (2) на c, получаем:

$$ac \equiv bc \pmod m. \tag{3}$$

Сопоставляя (3) с (1), имеем:

$$bc \equiv bd \pmod m,$$

откуда, имея в виду, что $(b, m) = 1$, получаем:

$$c \equiv d \pmod m.$$

135. По условию, $a^{100} \equiv 2 \pmod{73}$; умножив обе части этого сравнения на a, получаем:

$$a^{101} \equiv 2a \pmod{73}; \tag{1}$$

но, по условию,

$$a^{101} \equiv 69 \pmod{73}. \tag{2}$$

Из (1) и (2) следует, что

$$2a \equiv 69 \pmod{73}.$$

Теперь, прибавив в правой части модуль 73, будем иметь:

$$2a \equiv 142 \pmod{73}.$$

Так как $(2, 73) = 1$, то, сокращая члены сравнения на 2, получаем:

$$a \equiv 71 \pmod{73},$$

т. е. искомый остаток равен 71.

136. Из условия следует, что

$$11a + 2b \equiv 0 \pmod{19}.$$

Умножим обе части сравнения на 12:

$$132\,a + 24b \equiv 0 \pmod{19},$$

откуда

$$18\,a + 5\,b \equiv 0 \pmod{19}.$$

137. Составим из чисел

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

$\frac{p-1}{2}$ сравнений:

$$\left.\begin{array}{l} 1 \equiv -(p-1), \\ 2 \equiv -(p-2), \\ \cdots\cdots\cdots \\ \dfrac{p-1}{2} \equiv -\dfrac{p+1}{2}. \end{array}\right\} \pmod{p}$$

Возводя каждое из этих сравнений в степень $2k+1$ и складывая, получаем требуемое сравнение.

138. Если $a \equiv b \pmod{p^n}$, то $a = b + tp^n$ и потому

$$a^p = (b + tp^n)^p = b^p + pb^{p-1}tp^n + \ldots + t^p p^{np} = b^p + b^{p-1}tp^{n+1} + \ldots + t^p p^{np}.$$

Отсюда

$$a^p \equiv b^p \pmod{p^{n+1}}.$$

§ 10. Вычеты и системы вычетов

139. 1) По $m = 9$. Полные системы вычетов:
0, 1, 2, 3, 4, 5, 6, 7, 8; — 8, — 7, — 6, — 5, — 4, — 3, — 2, — 1, 0; — 4, — 3, — 2, — 1, 0, 1, 2, 3, 4.

Приведенные системы вычетов:
1, 2, 4, 5, 7, 8; — 8, — 7, — 5, — 4, — 2, — 1; — 4, — 2, — 1, 1, 2, 4.

2) По $m = 8$. Полные системы вычетов:
0, 1, 2, 3, 4, 5, 6, 7; — 7, — 6, — 5, — 4, — 3, — 2, — 1, 0; — 3, — 2, — 1, 0, 1, 2, 3, 4 или — 4, — 3, — 2, — 1, 0, 1, 2, 3.
Приведенные системы вычетов:
1, 3, 5, 7; — 7, — 5, — 3, — 1; — 3, — 1, 1, 3.

140. По общему виду всех чисел данного класса находим:

$25 = 8 \cdot 3 + 1$; $-20 = 8 \cdot (-3) + 4$; $16 = 8 \cdot 2 + 0$;
$46 = 8 \cdot 5 + 6$; $-21 = 8 \cdot (-3) + 3$; $18 = 8 \cdot 2 + 2$;
$37 = 8 \cdot 4 + 5$; $-17 = 8 \cdot (-3) + 7$.

Полученные остатки все различны и составляют полную систему наименьших неотрицательных вычетов 0, 1, 2, 3, 4, 5, 6, 7, следовательно, и данные числа представляют собой полную систему вычетов (только не наименьших).

Можно было бы найти неположительные остатки, наименьшие по абсолютной величине или абсолютно наименьшие.

147. Находим:

$24 = 6 \cdot 4 + 0$; $14 = 6 \cdot 2 + 2$; $25 = 6 \cdot 4 + 1$; $37 = 6 \cdot 6 + 1$; $-8 = 6 \cdot (-2) + 4$; $-19 = 6 \cdot (-4) + 5$; $-40 = 6 \cdot (-7) + 2$.

Выписываем остатки в найденном порядке: 0, 2, 1, 1, 4, 5, 2. Вычитая из каждого найденного неотрицательного вычета, кроме вычета нуль, величину модуля 6, получим 0, — 4, — 5, — 5, — 2, — 1, — 4 — наименьшие по абсолютной величине неположительные вычеты. Абсолютно наименьшими вычетами будут 0, 2, 1, 1, — 2, — 1, 2.

Все вычеты, значит, и данные числа принадлежат к пяти различным классам.

К одному и тому же классу принадлежат числа 14 и — 40 с одинаковыми вычетами 2 или — 4, а также числа 25 и 37 с вычетами 1 или — 5.

149. Наименьшие неотрицательные вычеты:

0, 2, 1, 0, 100, 100;

неположительные вычеты, наименьшие по абсолютной величине:

0, — 5, — 10, 0, — 20, — 100;

абсолютно наименьшие вычеты:

0, 2, 1, 0, — 20, 100 или — 100.

§ 11. Теоремы Эйлера и Ферма

152. 1) Так как $(5, 24) = 1$ и $\varphi(24) = 8$, то должно быть $5^8 \equiv 1 \pmod{24}$. Действительно, $5^8 = (5^2)^4 = 25^4 \equiv 1^4 = 1 \pmod{24}$.

4) Так как $(3, 18) = 3 > 1$, то теорема Эйлера не имеет места. Действительно, $\varphi(18) = 6$ и $3^6 = 3^4 \cdot 3^2 = 81 \cdot 9 \equiv 9 \cdot 9 = 81 \equiv 9 \pmod{18}$.

153. 1) Так как $\varphi(6) = 2$, то $a^2 \equiv 1 \pmod 6$. Удовлетворяют значения $a = 1$ и $a = 5$, взаимно простые с модулем 6, или классы чисел $6k + 1$ и $6k + 5$.

154. 1) Так как $383 \equiv 23 \pmod{45}$, то $383^{175} \equiv 23^{175} \pmod{45}$. Далее, так как $\varphi(45) = 24$ и $(23, 45) \equiv 1$, то по теореме Эйлера

$23^{24} \equiv 1 \pmod{45}$; следовательно, $23^{175} = 23^{24 \cdot 7 + 7} = (23^{24})^7 \cdot 23^7 \equiv 1^7 \cdot 23^7 \pmod{45}$, но $23^7 = (23^2)^3 \cdot 23 = 529^3 \cdot 23 \equiv 34^3 \cdot 23 = 34^2 \cdot 34 \cdot 23 = 1156 \cdot 782 \equiv 31 \cdot 17 = 527 \equiv 32 \pmod{45}$.

Итак, $383^{175} \equiv 32 \pmod{45}$. Искомый остаток равен 32.

2) 1. 3) 19. 4) 29.

155. 1) Так как $\varphi(11) = 10$ и $(3, 11) = 1$, то $3^{10} \equiv 1 \pmod{11}$ и $7^{10} \equiv 1 \pmod{11}$, поэтому $3^{80} = (3^{10})^8 \equiv 1^8 \equiv 1 \pmod{11}$ и $7^{80} = (7^{10})^8 \equiv 1 \pmod{11}$.

Сложив эти сравнения, получаем: $3^{80} + 7^{80} \equiv 2 \pmod{11}$, т. е. искомый остаток равен 2.

Другое решение. Так как $3 \equiv -8 \pmod{11}$, $7 \equiv -4 \pmod{11}$ и так как $\varphi(11) = 10$ и $(2, 11) = 1$, то $2^{10} \equiv 1 \pmod{11}$. Поэтому $3^{80} \equiv (-8)^{80} = 2^{240} = (2^{10})^{24} \equiv 1 \pmod{11}$ и $7^{80} = (-4)^{80} = 4^{80} = 2^{160} = (2^{10})^{16} \equiv 1 \pmod{11}$. После сложения получаем:

$$3^{80} + 7^{80} \equiv 2 \pmod{11}.$$

2) 6. 3) 2. 4) 2.

156. Число, выраженное последними двумя цифрами числа 2^{100}, получим как остаток от деления 2^{100} на 100. Имеем: $2^{100} = (2^{10})^{10} = 1024^{10} \equiv 24^{10} = (24^2)^5 = 576^5 \equiv 76^5 \equiv (-24)^5 = (-24)^4 \cdot (-24) = 576^2 \cdot (-24) \equiv (-24)^2 \cdot (-24) = 576 \cdot (-24) \equiv (-24)^2 = 576 \equiv 76 \pmod{100}$, т. е. искомые последние две цифры числа 2^{100} составляют число 76.

Другое решение. Так как $100 = 25 \cdot 4$, то воспользуемся теоремой Эйлера и возьмем сравнение: $2^{\varphi(25)} \equiv 1 \pmod{25}$, т. е. $2^{20} \equiv 1 \pmod{25}$. Так как $2^{100} = 2^{98} \cdot 2^2$, то найдем сначала остаток от деления 2^{98} на 25. Имеем: $2^{98} = 2^{80} \cdot 2^{18} = (2^{20})^4 \cdot (2^9)^2 \equiv 1^4 \cdot 12^2 = 144 \equiv 19 \pmod{25}$, отсюда $2^{98} = 25q + 19$. Умножив члены полученного равенства на 4, находим $2^{100} = 100q + 76$.

157. Число, выраженное последними тремя цифрами числа 243^{402}, получим как остаток от деления 243^{402} на 1000.

Так как $(243, 1000) = 1$ и $\varphi(1000) = 400$, то по теореме Эйлера $243^{400} \equiv 1 \pmod{1000}$. Поэтому $243^{402} = 243^{400} \cdot 243^2 \equiv 1 \cdot 59\,049 \equiv 49 \pmod{1000}$. Искомые последние три цифры 049.

158. Если положить остаток равным x, то будем иметь:

$$93^{41} \equiv x \pmod{111}.$$

Так как $(93, 111) = 3$, то $31 \cdot 93^{40} \equiv x_1 \pmod{37}$. Вычисление дает: $x_1 = 7$ и $x = 3x_1 = 21$.

159. Пусть $a^p - 1 = (a-1)(a^{p-1} + a^{p-2} + \ldots + a + 1) \equiv 0 \pmod{p}$. По следствию из теоремы Ферма $a^p \equiv a \pmod{p}$; поэтому

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

Таким образом, если $a^p - 1 \equiv 0 \pmod{p}$, то и $a - 1 \equiv 0 \pmod{p}$.

Но из последнего сравнения имеем:

$$\left.\begin{array}{l} a^{p-1} \equiv 1, \\ a^{p-2} \equiv 1, \\ \ldots\ldots \\ a \equiv 1, \\ 1 \equiv 1. \end{array}\right\} \pmod{p}$$

Складывая эти сравнения, получим:

$$a^{p-1} + a^{p-2} + \ldots + a + 1 \equiv p \equiv 0 \pmod{p}$$

и, следовательно, $a^p - 1 \equiv 0 \pmod{p^2}$.

Аналогично находим, что если $a^p + 1 \equiv 0 \pmod{p}$, то $a^p + 1 \equiv 0 \pmod{p^2}$.

160. По теореме Ферма:

$$p^{q-1} - 1 \equiv 0 \pmod{q},$$

откуда

$$p^{q-1} - 1 = qt_1, \tag{1}$$

Аналогично имеем:

$$q^{p-1} - 1 \equiv 0 \pmod{p},$$

откуда

$$q^{p-1} - 1 = pt_2. \tag{2}$$

Перемножая (1) и (2), получаем искомое сравнение.

161. По следствию из теоремы Ферма $x^7 \equiv x \pmod 7$, а по теореме Эйлера $x^2 \equiv 1 \pmod 6$. Последнее сравнение можно представить как

$$\left.\begin{matrix} x^6 \equiv 1, \\ x^7 \equiv x \end{matrix}\right\} \pmod 6.$$

Но $(7,6) = 1$, следовательно, $x^7 \equiv x \pmod{42}$.

162. Имеем:

$$m - \left[\frac{m}{2}\right] = m - \frac{m-1}{2} = \frac{m+1}{2}.$$

Пусть при делении $2^{\varphi(m)-1}$ на m остаток равен r:

$$2^{\varphi(m)-1} \equiv r \pmod m,$$

или

$$2^{\varphi(m)} - 1 \equiv 2r - 1 \pmod m.$$

Но по теореме Эйлера $2^{\varphi(m)} - 1 \equiv 0 \pmod m$. Следовательно, и $2r - 1 \equiv 0 \pmod m$, что дает

$$2r - 1 = mt, \quad r = \frac{mt+1}{2}, \quad r = \frac{m+1}{2}.$$

163. Если остаток r, то, обращаясь к теореме Эйлера, получаем, что $4r \equiv 1 \pmod m$. Всякое нечетное число можно представить в одной из двух форм $m = 4k \pm 1$.

Пусть $m = 4k - 1$, тогда последнее сравнение можно написать как

$$4r \equiv 1 + m = 4k \pmod m,$$

отсюда

$$r = k = \frac{m+1}{4} = \left[\frac{m}{4}\right] + 1.$$

Если $m = 4k + 1$, то

$$4r \equiv 1 + 3m = 1 + 12k + 3 \pmod m,$$

$$r \equiv 3k + 1 \pmod{m},$$

$$r = 3k + 1 = \frac{3m + 1}{4} = m - \frac{m - 1}{4} = m - \left[\frac{m}{4}\right].$$

164. Составим разность:

$$M - N = (a_1^5 - a_1) + (a_2^5 - a_2) + \ldots + (a_n^5 - a_n).$$

По следствию из теоремы Ферма:

$$a_i^5 - a_i \equiv 0 \pmod 5.$$

В то же время

$$a_1^5 - a_i = (a_i - 1)\, a_i\, (a_i + 1)\, P \equiv 0 \pmod 6.$$

Итак,

$$M \equiv N \pmod{30}.$$

Но, по условию, $N \equiv 0 \pmod{30}$, значит,

$$M \equiv 0 \pmod{30}.$$

165. Если целое число a кратно 5, то $a = 5k$ и тогда

$$a^{100} = 5^{100} k^{100} \equiv 0 \pmod{125}.$$

Если же $(a, 5) = 1$, то по теореме Эйлера $a^{\varphi(125)} \equiv 1 \pmod{125}$, или $a^{100} \equiv 1 \pmod{125}$.

166. По условию, $(a, 10) = 1$, но тогда $(a, 5) = 1$ и $(a, 2) = 1$. Имея в виду, что $1000 = 125 \cdot 8$, используем сравнения по модулю 125 и по модулю 8.

Из решения задачи **165**:

$$a^{100} \equiv 1 \pmod{125}. \qquad (1)$$

С другой стороны, по теореме Эйлера $a^4 \equiv 1 \pmod 8$; возвысив это сравнение в 25-ю степень, получим:

$$a^{100} \equiv 1 \pmod 8. \qquad (2)$$

Теперь из (1) и (2) по третьему особому свойству сравнений следует:

$$a^{100} \equiv 1 \pmod{1000}.$$

Возведя это сравнение в n-ю степень и затем умножая обе части полученного сравнения на a, будем иметь:

$$a^{100n+1} \equiv a \pmod{1000}.$$

167. Используем сравнения по модулю 19 и по модулю 73, имея в виду, что $19 \cdot 73 - 1 = 1386 = 18 \cdot 77$.

По теореме Ферма $2^{18} \equiv 1 \pmod{19}$; возведем это сравнение в 77-ю степень:

$$2^{18 \cdot 77} = 2^{19 \cdot 73 - 1} \equiv 1 \pmod{19}. \qquad (1)$$

Далее, возьмем сравнение $2^9 = 512 \equiv 1 \pmod{73}$ и возведем его в 154-ю степень:

$$2^{9 \cdot 154} = 2^{19 \cdot 73 - 1} \equiv 1 \pmod{73}. \qquad (2)$$

Теперь из (1) и (2) по третьему особому свойству сравнений получаем:

$$2^{19\cdot 73-1} \equiv 1 \pmod{19\cdot 73}.$$

168. Если a не кратно 7, то $(a, 7) = 1$ и по теореме Ферма

$$a^6 \equiv 1 \pmod 7.$$

Возведем это сравнение в степень m и в степень n:

$$a^{6m} \equiv 1 \pmod 7 \quad \text{и} \quad a^{6n} \equiv 1 \pmod 7.$$

Складывая их, получим:

$$a^{6m} + a^{6n} \equiv 2 \pmod 7,$$

т. е. при всех a, не кратных 7, двучлен $a^{6m} + a^{6n}$ при делении на 7 дает в остатке 2, а не нуль, что и требовалось показать.

169. Если $(n, 6) = 1$, то $(n, 2) = 1$. Отсюда следует, что n — число нечетное, значит, $(n - 1)(n + 1)$ делится на 8 как произведение двух последовательных четных чисел, т. е. имеем:

$$n^2 - 1 \equiv 0 \pmod 8, \text{ или } n^2 \equiv 1 \pmod 8.$$

С другой стороны, из условия $(n, 6) = 1$ следует, что $(n, 3) = 1$, поэтому мы можем по теореме Ферма написать сравнение:

$$n^2 \equiv 1 \pmod 3. \qquad (2)$$

Теперь из (1) и (2) по третьему особому свойству сравнений получаем:

$$n^2 \equiv 1 \pmod{24},$$

что и требовалось показать.

170. Действительно, при $p = 3$ число $8p^2 + 1 = 73$ является тоже простым.

Теперь предположим, что $p \neq 3$. В таком случае $(p, 3) = 1$, тогда по теореме Ферма имеем сравнение: $p^2 \equiv 1 \pmod 3$. Умножив члены этого сравнения на 8 и сложив с очевидным сравнением $1 \equiv 1 \pmod 3$, получаем сравнение:

$$8p^2 + 1 \equiv 9 \equiv 0 \pmod 3,$$

из которого следует, что число $8p^2 + 1$ делится на 3, т. е. является составным.

171. Искомое простое число $p \neq 5$, так как $5^{25} + 1 \not\equiv 0 \pmod{25}$ (второе слагаемое 1 не делится на 25).

Для решения задачи преобразуем сравнение так:

$$5^{p^2} + 1 = \left(5^{p^2} - 5\right) + 6 = 5\left(5^{p^2-1} - 1\right) + 6 = 5\left[(5^{p-1})^{p+1} - 1\right] + 6 \equiv 0 \pmod{p^2}.$$

Число $(5^{p-1})^{p+1} - 1$ кратно $5^{p-1} - 1$, а при $p = 5$ имеем: по теореме Ферма $5^{p-1} - 1 \equiv 0 \pmod p$, следовательно, и второе слагаемое 6 делится на p. Отсюда $p = 2$ или $p = 3$. Значение $p = 2$ непригодно, так как $5^{2^2} + 1 = 626 \not\equiv 0 \pmod{2^2}$. При $p = 3$ получаем:

$$5^{3^2} + 1 = 1\,953\,126 \equiv 0 \pmod{3^2},$$

следовательно, искомое число $p = 3$.

172. Надо доказать, что $(x^3 - 1)\, x^3 (x^3 + 1) \equiv 0 \pmod{504}$, или, что то же, $x^2 (x^7 - x) \equiv 0 \pmod{7 \cdot 8 \cdot 9}$. Но по следствию из теоремы Ферма $x^7 - x \equiv 0 \pmod 7$ при любом целом значении x, следовательно, и

$$(x^3 - 1)\, x^3 (x^3 + 1) \equiv 0 \pmod 7; \qquad (1)$$

в то же время

$$(x^3 - 1)\, x^3 (x^3 + 1) \equiv 0 \pmod 8, \qquad (2)$$

как при x четном, так и нечетном, и так как $\varphi(9) = 6$, то

$$x^3 (x^6 - 1) \equiv 0 \pmod 9. \qquad (3)$$

Таким образом, из (1), (2), (3) по третьему особому свойству сравнений получаем:

$$(x^3 - 1)\, x^3 (x^3 + 1) \equiv 0 \pmod{504}.$$

173. По условию, числа p и $2p + 1$ — простые, поэтому по теореме Ферма имеем сравнения:

$$(2p + 1)^2 \equiv 1 \pmod 3, \qquad (1)$$
$$p^2 \equiv 1 \pmod 3. \qquad (2)$$

Теперь, умножая (2) на 4 и вычитая из (1), получаем:

$$4p + 1 \equiv -3 \equiv 0 \pmod 3,$$

откуда следует, что $4p + 1$ — составное (делится на 3).

§ 12. Сравнения с одним неизвестным (общие понятия)

174. 1) Испытывая числа 0, 1, 2, составляющие полную систему наименьших неотрицательных вычетов по модулю 3, находим, что сравнению удовлетворяют числа 1 и 2, т. е. получаем решения:

$$\left.\begin{aligned} x_1 &\equiv 1, \\ x_2 &\equiv 2, \end{aligned}\right\} \pmod 3$$

или классы чисел $x_1 = 3k + 1$ и $x_2 = 3k + 2$, которые дают числа:

$$\ldots, -8, -5, -2, 1, 4, 7, \ldots$$
$$\ldots, -7, -4, -1, 2, 5, 8, \ldots .$$

2) $\left.\begin{aligned} x_1 &\equiv 1, \\ x_2 &\equiv 2, \end{aligned}\right\} \pmod 5$, или классы чисел $x_1 = 5k + 1$, $x_2 = 5k + 2$.
3) $x \equiv 2 \pmod 5$, или класс чисел $x = 5k + 2$.
5) Решения нет.
9) $x \equiv 3 \pmod 5$, или класс чисел $x = 5k + 3$.

175. 1) Исключая $7x$ из левой части сравнения, по второму следствию из второго основного свойства сравнений получаем сравнение:

$$5x \equiv 1 \pmod 7.$$

Путем испытаний находим решение:

$$x \equiv 3 \pmod 7.$$

3) Исключая 11 из 13, по второму следствию из второго основного свойства, получаем сравнение:

$$3x \equiv 2 \pmod{11}.$$

Путем испытаний находим решение:

$$x \equiv 8 \pmod{11}.$$

4) Так как $(3,7) = 1$, то, по четвертому основному свойству, деля члены сравнения на 3, получаем сравнение:

$$2x \equiv 1 \pmod{7}.$$

Путем испытаний находим решение:

$$x \equiv 4 \pmod{7}.$$

6) Применяя первое следствие из второго свойства, затем четвертое свойство, получаем сравнение $2x \equiv 1 \pmod{7}$. Путем испытаний находим решение:

$$x \equiv 4 \pmod{7}.$$

9) Заменяя коэффициенты наименьшими неотрицательными вычетами по модулю 15, получаем сравнение:

$$x^2 - 7x + 1 \equiv 0 \pmod{15}.$$

Испытаниями находим решение $x \equiv -4 \pmod{15}$.

176. 1) Прибавляя к правой части сравнения число 15, равное модулю, получаем сравнение $2x \equiv 22 \pmod{15}$; так как $(2,15) = 1$, то, сокращая обе части сравнения на 2, получаем решение:

$$x \equiv 11 \pmod{15}.$$

177. Введя подстановку $x = y + \alpha$, получаем:

$$(y + \alpha)^n + a_1 (y + \alpha)^{n-1} + \ldots + a_n \equiv 0 \pmod{m}.$$

После преобразований будем иметь:

$$y^n + (n\alpha + a_1)\, y^{n-1} + \ldots + (\alpha^n + a_1\alpha^{n-1} + \ldots + a_n) \equiv 0 \pmod{m}. \quad (1)$$

Выбираем α такое, чтобы было

$$n\alpha + a_1 \equiv 0 \pmod{m}. \quad (2)$$

В результате член, содержащий y^{n-1}, исключается из сравнения (1), и мы получим сравнение:

$$y^n + b_2 y^{n-2} + \ldots + b_n \equiv 0 \pmod{m}.$$

178. Составляем сравнение $n\alpha + a_1 \equiv 0 \pmod{m}$. Из условия имеем: $3\alpha + 5 \equiv 0 \pmod{13}$, его решение: $\alpha \equiv 7 \pmod{13}$; следовательно, для подстановки берем $x = y + 7$. Подставляя в сравнение, получаем:

$$(y + 7)^3 + 5(y + 7)^2 + 6(y + 7) - 8 = y^3 + 26y^2 + 223y + 622 \equiv y^3 + 2y - 2 \equiv 0 \pmod{13}.$$

§ 13. Сравнения первой степени

179. 3) **Решения нет, так как** $(5,10) = 5$, **но 7 не делится на 5.**
4) По формуле $x \equiv ba^{\varphi(m)-1} \pmod m$ находим:
$x = 8 \cdot 3^{11} = 8 \cdot 3^3 \cdot (3^4)^2 = 216 \cdot 81^2 \equiv 8 \cdot 3^3 = 72 \equiv 7 \pmod{13}$.

Проверка. $3 \cdot 7 \equiv 8 \pmod{13}$.

180. 1) Находим необходимые данные для формулы:

$$x = (-1)^n bP_{n-1} \pmod m.$$

Имеем:

$$\begin{array}{r|l} 19 & 7 \\ \hline 7 & 5 \quad 2=q_0 \\ \hline 5 & 2 \quad 1=q_1 \\ \hline 2 & 1 \quad 2=q_2 \\ \hline & 2=q_3 \end{array}$$

q			2	1	2	2
P	0	1	2	3	8	19

$$n = 3, \quad P_{n-1} = 8.$$

Отсюда $x \equiv (-1)^3 \cdot 4 \cdot 8 = -32 \equiv -13 \equiv 6 \pmod{19}$.

Проверка. $7 \cdot 6 \equiv 4 \pmod{19}$.

7) Решения нет, так как $(143, 221) = 13$, но 41 не делится на 13.

181. 2) Сравнение неразрешимо, так как $(12,18) = 6$, но 9 не делится на 6.

3) Так как $(20, 10, 25) = 5$, то после сокращения членов сравнения и модуля его на 5 получаем сравнение:

$$4x \equiv 2 \pmod 5, \text{ или } 2x \equiv 1 \pmod 5.$$

Способом испытаний находим: $x \equiv 3 \pmod 5$.
Теперь по формуле $x_{k+1} \equiv m_1 k + \alpha \pmod m$ имеем:

$$x_1 \equiv 3, \quad x_2 \equiv 8, \quad x_3 \equiv 13, \quad x_4 \equiv 18, \quad x_5 \equiv 23 \pmod{25}.$$

Проверка. $20 \cdot 3 - 10 = 50$ делится на 25; $20 \cdot 8 - 10 = 150$ делится на 25; $20 \cdot 13 - 10 = 250$ делится на 25; $20 \cdot 18 - 10 = 350$ делится на 25; $20 \cdot 23 - 10 = 450$ делится на 25.

182. Обозначим приписываемое число через x, тогда

$$523 \cdot 10^3 + x \equiv 0 \pmod{7 \cdot 8 \cdot 9},$$

откуда

$$x \equiv -523\,000 \equiv -352 \equiv 152 \pmod{504},$$

или класс чисел

$$x = 504t + 152.$$

Значение x будет трехзначным числом при $t = 0$ и $t = 1$.
Получаем: $x_1 = 152$; $x_2 = 656$.

Проверка. 523 152 делится на 7, 8, 9; 523 656 делится на 7, 8, 9.

§ 14. Системы сравнений первой степени

184. 1) По условию, $x \equiv 4 \pmod 5$, $x \equiv 1 \pmod{12}$, $x \equiv 7 \pmod{14}$. Из первого сравнения имеем:

$$x = 5t + 4. \tag{1}$$

Подставляем во второе сравнение: $5t + 4 \equiv 1 \pmod{12}$, или $5t \equiv 9 \pmod{12}$, откуда $t \equiv 9 \pmod{12}$, или $t = 12t_1 + 9$. Подставляя найденное значение t в равенство (1), находим:

$$x = 5(12t_1 + 9) + 4 = 60t_1 + 49. \tag{2}$$

Найденное значение x подставляем в третье сравнение: $60t_1 + 49 \equiv 7 \pmod{14}$, или $60t_1 \equiv -42 \pmod{14}$, или $4t_1 \equiv 0 \pmod{14}$. Сокращая члены сравнения и модуль на 2, получаем: $2t_1 \equiv 0 \pmod 7$, или $t_1 \equiv 0 \pmod 7$, откуда $t_1 = 7t_2 + 0$. Подставляя найденные значения t_1 в равенство (2), находим:

$$x = 60(7t_2 + 0) + 49 = 420t_2 + 49.$$

Проверка. 49 — 4 делится на 5; 49 — 1 делится на 12; 49 — 7 делится на 14.

Замечание. Решая сравнение $4t \equiv 0 \pmod{14}$, мы получили сравнение $2t_1 \equiv 0 \pmod 7$, и решение его $t_1 \equiv 0 \pmod 7$, или $t_1 \equiv 7t_2 + 0$, которое привело к решению $x = 420t_2 + 49$ данной в условии системы. Но сравнение $4t_1 \equiv 0 \pmod{14}$ имеет еще второе решение $t_1 \equiv 7 \pmod{14}$, или $t_1 = 14t_2 + 0$, поскольку $d = (4,14) = 2$, которое при подстановке в равенство (2) дает решение $x = 840t_2 + 469$. Однако $469 \equiv 49 \pmod{420}$, т. е. числа 469 и 49 принадлежат одному классу по модулю 420, поэтому мы не находим это второе решение системы.

Вообще, если какое-либо сравнение системы или сравнение относительно t_i имеет d решений по некоторому модулю m, то для решения системы достаточно ограничиться только решением равносильного ему сравнения по модулю $\frac{m}{d}$.

3) По условию, $k \equiv 1 \pmod{25}$; $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 7$, $x \equiv 4 \pmod 9$. Модули сравнений данной системы попарно просты, поэтому решение ее можно найти по формуле:

$$x_0 = \frac{M}{m_1} y_1 a_1 + \frac{M}{m_2} y_2 a_2 + \frac{M}{m_3} y_3 a_3 + \frac{M}{m_4} y_4 a_4.$$

Находим: $M = 6300$, $\frac{M}{m_1} = 252$, $\frac{M}{m_2} = 1575$, $\frac{M}{m_3} = 900$, $\frac{M}{m_4} = 700$.

Составляем сравнения: $252\, y_1 \equiv 1 \pmod{25}$, $1575\, y_2 \equiv 1 \pmod 4$, $900\, y_3 \equiv 1 \pmod 7$, $700\, y_4 \equiv 1 \pmod 9$, откуда $y_1 = -12$, $y_2 = -1$, $y_3 = 2$, $y_4 = 4$. Теперь по формуле находим: $x_0 = 252 \cdot (-12) \cdot 1 + 1575 \cdot (-1) \cdot 2 + 900 \cdot 2 \cdot 3 + 700 \cdot 4 \cdot 4 = -3024 - 3150 + 5400 + 11\,200 = 10\,426 \equiv 4126 \pmod{6300}$.

Итак, $x \equiv 4126 \pmod{6300}$.

Проверкой убеждаемся, что найденное значение x удовлетворяет сравнениям системы.

5) $x \equiv 85\,056 \pmod{130\,169}$.

6) $x \equiv 9573 \pmod{13\,923}$.

7) По условию, $3x \equiv 7 \pmod{10}$, $2x \equiv 5 \pmod{15}$, $7x \equiv 5 \pmod{12}$. Из первого сравнения имеем: $x \equiv 9 \pmod 7$, или

$$x = 10t + 9. \qquad (1)$$

Подставляем это значение x во второе сравнение и решаем его относительно t:

$$2(10t + 9) \equiv 5 \pmod{15},\ 20t \equiv -13 \pmod{15},\ 5t \equiv 2 \pmod{15}, \qquad (2)$$

но $(5,15) = 5$ и 2 не делится на 5, поэтому сравнение (2) относительно t неразрешимо, значит, не имеет решений и данная система сравнений.

8) Из данной системы сравнений видим, что в третьем сравнении $(4,12) = 4$, но 5 не делится на 4, поэтому оно неразрешимо; следовательно, не решая систему, можно сказать, что она не имеет решений.

9) Решений нет.

10) По условию, $3x \equiv 1 \pmod{10}$, $4x \equiv 3 \pmod 5$, $2x \equiv 7 \pmod 9$. Из первого сравнения имеем: $x \equiv 7 \pmod{10}$, или

$$x = 10t + 7. \qquad (1)$$

Подставляя во второе сравнение, получаем: $4(10t + 7) \equiv 3 \pmod 5$, $40t \equiv -25 \pmod 5$. Так как коэффициенты полученного сравнения кратны 5, то оно имеет место при любом значении t; иначе говоря, это сравнение не накладывает никаких ограничений на значение x из второго сравнения системы. Поэтому продолжаем решение, подставляя значение x из (1) в третье сравнение системы:

$2(10t + 7) \equiv 7 \pmod 9$, $20t \equiv -7 \pmod 9$, $2t \equiv \pmod 9$, $t \equiv 1 \pmod 9$, или $t \equiv 9t_1 + 1$. Найденное значение подставляем в равенство (1) и находим:

$$x = 10(9t_1 + 1) + 7 = 90t_1 + 17, \text{ т. е. } x \equiv 17 \pmod{90}.$$

Проверка. $3 \cdot 17 - 1 = 50$ делится на 10; $4 \cdot 17 - 3 = 65$ делится на 5; $2 \cdot 17 - 7 = 27$ делится на 9.

185. 262.

186. 1) По условию, $x \equiv 5 \pmod{18}$, $x \equiv 8 \pmod{21}$, $x \equiv a \pmod{35}$. Из первого сравнения имеем:

$$x = 18t + 5; \qquad (1)$$

подставляем x во второе сравнение и находим t: $18t + 5 \equiv 8 \pmod{21}$, $18t \equiv 3 \pmod{21}$, $6t \equiv 1 \pmod 7$, $t \equiv 6 \pmod 7$, или удобнее взять $t \equiv -1 \pmod 7$, откуда $t = 7t_1 - 1$. Подставляем найденное значение t в равенство (1):

$$x = 16(7t_1 - 1) + 5 = 126t_1 - 13.$$

Это значение x подставляем в третье сравнение системы:

$$126t_1 - 13 \equiv a \pmod{35}, \text{ т. е.}$$
$$21t_1 \equiv a + 13 \pmod{35}. \qquad (2)$$

Так как $(21,35) = 7$, то для разрешимости сравнения (2) необходимо иметь $a + 13 \equiv 0 \pmod 7$, или $a \equiv 1 \pmod 7$, что и будет условием совместности данной системы.

2) $a \equiv 1 \pmod 6$.

187. Из условия имеем систему сравнений:

$$4x\ 87y6 \equiv 0 \pmod 8, \quad 4x87y6 \equiv 0 \pmod 7.$$

Из первого сравнения по признаку делимости на 8 следует, что $7y6$ делится на 8, что будет при $y = 3$ и $y = 7$.

Подставляя во второе сравнение, получаем:

$$4x8736 \equiv 0 \pmod 7, \quad 4x8776 \equiv 0 \pmod 7.$$

Представим полученные сравнения так:

$$400\,000 + 10\,000x + 8736 \equiv 0 \pmod 7,$$
$$400\,000 + 10\,000x + 8776 \equiv 0 \pmod 7,$$

или после упрощений

$$4x \equiv 1 \pmod 7, \quad 4x \equiv 3 \pmod 7.$$

Первое сравнение имеет решение $x \equiv 2 \pmod 7$, или $x = 7t + 2$, откуда при $t = 0$ получаем $x_1 = 2$ и при $t = 1$ будет $x_2 = 9$. При других t значения x не пригодны.

Второе сравнение имеет решение $x \equiv 6 \pmod 7$, или $x = 7t + 6$, откуда получаем единственное значение $x_3 = 6$. Подставляя найденные значения x, получаем числа: 428 736, 498 736, 468 776.

188. Из условия имеем систему сравнений:

$$\left.\begin{aligned} xyz138 &\equiv 0 \pmod 7,\\ 138xyz &\equiv 6 \pmod{13},\\ x1y3z8 &\equiv 5 \pmod{11}. \end{aligned}\right\}$$

Первое сравнение запишем так:

$$10^3xyz + 138 \equiv 0 \pmod 7.$$

Упростив его, получаем $3xyz \equiv 1 \pmod 7$, откуда

$$xyz \equiv 5 \pmod 7. \tag{1}$$

Аналогично поступая со вторым сравнением, будем иметь: $138\,000 + xyz \equiv 6 \pmod{13}$, откуда

$$xyz \equiv 1 \pmod{13}. \tag{2}$$

Решая систему сравнений (1) и (2) относительно xyz, получаем $xyz \equiv 40 \pmod{91}$, или $xyz = 91t + 40$. Полагая $t = 1, 2, 3, \ldots, 10$, находим:

$$xyz = 131,\ 222,\ 313,\ \ldots,\ 950. \tag{3}$$

Теперь третье сравнение системы представим так:

$$x \cdot 10^5 + 10^4 + y \cdot 10^3 + 3 \cdot 10^2 + z \cdot 10 + 8 \equiv 5 \pmod{11},$$

или после упрощений $x + y + z \equiv 7 \pmod{11}$, т. е.

$$x + y + z = 11t + 7. \tag{4}$$

Учитывая, что $0 < x + y + z < 27$, из (4) имеем:

$$x + y + z = 7 \quad \text{и} \quad x + y + z = 18.$$

Обращаясь к ряду чисел в равенстве (3), находим два числа, удовлетворяющие условию: 313 138 и 495 138.

189. Решение распадается на два случая.

Первый случай. Пусть $x+1$ — число, выраженное первыми четырьмя цифрами, а x — число, выраженное последними четырьмя цифрами, и, следовательно,

$$N^2 = 10^4(x+1) + x = 10\,001x + 10\,000,$$

откуда

$$x = \frac{N^2 - 10\,000}{10\,001} = \frac{(N+100)(N-100)}{73 \cdot 137},$$

что дает две системы:

$$\left.\begin{aligned} &1)\ N+100 \equiv 0 \pmod{73},\\ &\ \ N-100 \equiv 0 \pmod{137}; \end{aligned}\right\} \qquad \left.\begin{aligned} &2)\ N+100 \equiv 0 \pmod{137},\\ &\ \ N-100 \equiv 0 \pmod{73}. \end{aligned}\right\}$$

Значение N из первой системы не удовлетворяет условию задачи, так как в этом случае N^2 — шестизначное число. Решая вторую систему, получаем $N = 9079$ и $N^2 = 82\,428\,241$.

Может также быть $N + 100 = 73 \cdot 137$, тогда $N = 9901$ и $N^2 = 98\,029\,801$.

$N - 100 = 73 \cdot 137$ не удовлетворяет условию задачи, так как N^2 — девятизначное число.

Второй случай. Пусть x — число, выраженное первыми четырьмя цифрами, а $x+1$ — число, выраженное последними четырьмя цифрами, и, следовательно, $N^2 = 10^4 x + (x+1) = 10\,001x + 1$, откуда

$$x = \frac{N^2 - 1}{10\,001} = \frac{(N+1)(N-1)}{73 \cdot 137},$$

что дает две системы:

$$\left.\begin{aligned} &1)\ N+1 \equiv 0 \pmod{73},\\ &\ \ N-1 \equiv 0 \pmod{137}; \end{aligned}\right\} \qquad \left.\begin{aligned} &2)\ N+1 \equiv 0 \pmod{137},\\ &\ \ N-1 \equiv 0 \pmod{73}. \end{aligned}\right\}$$

Решая первую систему, получаем $N = 7810$ и $N^2 = 60\,996\,100$.

Значение N из второй системы не удовлетворяет условию задачи, так как N^2 — семизначное число.

Значения $N + 1 = 73 \cdot 137$ и $N - 1 = 73 \cdot 137$ не удовлетворяют условию задачи.

190. По условию, $13xy45z \equiv 0 \pmod{792}$, но $792 = 8 \cdot 9 \cdot 11$, поэтому можно написать систему:

$$\left.\begin{aligned} &13xy45z \equiv 0 \pmod 8,\\ &13xy45z \equiv 0 \pmod 9,\\ &13xy45z \equiv 0 \pmod{11}. \end{aligned}\right\}$$

Из первого сравнения по признаку делимости на 8 имеем:

$$450 + z \equiv 0 \pmod 8, \quad \text{откуда} \quad z \equiv 6 \pmod 8.$$

Подставляя $z = 6$ во второе и третье сравнения, получаем систему:

$$\left.\begin{aligned} &13xy456 \equiv 0 \pmod 9,\\ &13xy456 \equiv 0 \pmod{11}. \end{aligned}\right\}$$

Из первого сравнения этой системы по признаку делимости на 9 имеем $x + y + 19 \equiv 0 \pmod 9$, или

$$x + y \equiv 0 \pmod 9. \qquad (1)$$

Второе сравнение системы представим так: $1\,300\,000 + x \cdot 10^4 + y \cdot 10^3 + 456 \equiv 0 \pmod{11}$, или после упрощения

$$x - y \equiv 8 \pmod{11}. \qquad (2)$$

Из сравнений (1) и (2) имеем:

$$\left.\begin{aligned} x + y &= 9t_1 + 8, \\ x - y &= 11t_2 + 8. \end{aligned}\right\}$$

Теперь легко видеть, что $x = 8$ и $y = 0$. Итак, искомое число 1 380 456.

191. Обозначив искомое трехзначное число через x, по условию имеем:

$$x \cdot 1000 + (x + 1) = 1001x + 1 = N^2,$$

или

$$(N + 1)(N - 1) = 7 \cdot 11 \cdot 13\, x,$$

откуда

$$x = \frac{(N + 1)(N - 1)}{7 \cdot 11 \cdot 13}.$$

Из этого равенства для определения N и x имеем ряд систем:

1) $\left.\begin{aligned} N + 1 &\equiv 0 \pmod 7, \\ N - 1 &\equiv 0 \pmod{143}. \end{aligned}\right\}$

Решая систему обычным путем, находим $N = 573$, $N^2 = 328\,329$, $x_1 = 328$.

2) $\left.\begin{aligned} N + 1 &\equiv 0 \pmod{143}, \\ N - 1 &\equiv 0 \pmod 7, \end{aligned}\right\}$

откуда $N = 428$, $N^2 = 183\,184$, $x_2 = 183$.

3) $\left.\begin{aligned} N + 1 &\equiv 0 \pmod{11}, \\ N - 1 &\equiv 0 \pmod{91}, \end{aligned}\right\}$

откуда $N = 274$, $N^2 = 075\,076$, но $x = 075$ не является решением, как число двузначное.

4) $\left.\begin{aligned} N + 1 &\equiv 0 \pmod{91}, \\ N - 1 &\equiv 0 \pmod{11}. \end{aligned}\right\}$

Получаем $N = 727$, $N^2 = 528\,529$, $x_3 = 528$.

5) $\left.\begin{aligned} N + 1 &\equiv 0 \pmod{13}, \\ N - 1 &\equiv 0 \pmod{77}. \end{aligned}\right\}$

$N = 155$, $N^2 = 024\,025$, но $x = 025$ не является решением, как число двузначное.

6) $\left.\begin{aligned} N + 1 &\equiv 0 \pmod{77}, \\ N - 1 &\equiv 0 \pmod{13}, \end{aligned}\right\}$

откуда $N = 846$, $N^2 = 715\,716$, $x_4 = 715$.

192. Из условия получаем систему:

$$\left.\begin{aligned} x &\equiv 3 \pmod 7, \\ x^2 &\equiv 44 \pmod{7^2}, \\ x^3 &\equiv 111 \pmod{7^3}. \end{aligned}\right\}$$

Из первого сравнения имеем:

$$x = 7t + 3. \tag{1}$$

Подставляем найденное значение x во второе сравнение и решаем последнее относительно t: $(7t + 3)^2 = 44 \pmod{7^2}$, или, после упрощения,

$$42t \equiv 35 \pmod{7^2}.$$

Сокращая на 7, получаем $6t \equiv 5 \pmod 7$, откуда $t \equiv 2 \pmod 7$; это дает $t = 7t_1 + 2$. Подставляем это значение t в равенство (1):

$$x = 7(7t_1 + 2) + 3 = 49t_1 + 17. \tag{2}$$

Теперь, подставляя x в третье сравнение системы, имеем:

$$(49t_1 + 17)^3 \equiv 111 \pmod{7^3}.$$

После возвышения в куб и упрощения находим:

$$t_1 \equiv 0 \pmod 7, \text{ откуда } t_1 = 7t_2 + 0.$$

Подставляя это значение t_1 в равенство (2), окончательно получаем $x = 17 \pmod{7^3}$.

193. Сравнение $x^2 \equiv -1 \pmod{65}$ равносильно системе:

$$\left.\begin{aligned} x^2 &\equiv -1 \pmod 5, \\ x^2 &\equiv -1 \pmod{13}. \end{aligned}\right\}$$

Путем испытаний абсолютно наименьших вычетов находим решения соответственно первого и второго сравнений:

$$x \equiv \pm 2 \pmod 5,$$

$$x \equiv \pm 5 \pmod{13}.$$

Теперь, решая четыре системы:

$$\left.\begin{aligned} x &\equiv \pm 2 \pmod 5, \\ x &\equiv \pm 5 \pmod{13}, \end{aligned}\right\}$$

получаем четыре решения данного сравнения:

$$x \equiv \pm 8, \pm 18 \pmod{65}.$$

§ 15. Решение в целых числах неопределенных уравнений первой степени с двумя неизвестными при помощи сравнений

194. 1) Из уравнения имеем сравнение $3x \equiv 13 \pmod 4$, или $3x \equiv 1 \pmod 4$, откуда $x_1 = 3$. Подстановкой в уравнение находим $y_1 = 1$. Общим решением будет:

$$x = 3 + 4t,$$
$$y = 1 - 3t.$$

2) $\left.\begin{aligned} x &= 3 + 13t, \\ y &= -3 + 8t. \end{aligned}\right\}$ 6) $\left.\begin{aligned} x &= 22 - 37t, \\ y &= -25 + 43t. \end{aligned}\right\}$

4) $\left.\begin{aligned} x &= 20 + 22t, \\ y &= 35 + 39t. \end{aligned}\right\}$ 8) $\left.\begin{aligned} x &= 17 + 37t, \\ y &= 20 + 45t. \end{aligned}\right\}$

9) Предварительно сокращаем коэффициенты на 3, дальнейшее решение дает $x_1 = 1$ и $y_1 = 1$. Общим решением будет:

$$x = 1 + 16t,$$
$$y = 1 + 27t.$$

10) Так как $(26, 34) = 2$, а 13 не делится на 2, то данное уравнение неразрешимо в целых числах.

195. Из условия имеем уравнение $60x + 80y = 440$, или после сокращения на 20: $3x + 4y = 22$. Пишем сравнение $3x \equiv 22 \pmod 4$, или $3x \equiv 2 \pmod 4$, откуда $x_1 = 2$. Подстановкой в уравнение находим $y_1 = 4$. Общим решением будет:

$$x = 2 - 4t,$$
$$y = 4 + 3t.$$

При $t = 0$ и $t = -1$ получаем решения задачи.

197. $x = 3 - 5t$, $y = 28 + 3t$.

§ 16. Сравнения высших степеней по простому модулю

199. 1) Данное сравнение $6x^{10} - 12x + 1 \equiv 0 \pmod 5$ можно предварительно упростить, исключив из коэффициентов числа, кратные модулю. Получим сравнение:

$$x^{10} - 2x + 1 \equiv 0 \pmod 5.$$

Теперь, разделив $x^{10} - 2x + 1$ на $x^5 - x$, получим в остатке $x^2 - 2x + 1$. Пишем сравнение, равносильное данному: $x^2 - 2x + 1 \equiv 0 \pmod 5$. Непосредственными испытаниями абсолютно наименьших вычетов $0, \pm 1, \pm 2$ по модулю 5 находим решение $x \equiv 1 \pmod 5$.

Проверка. $6 \cdot 1^{10} - 12 \cdot 1 + 1 = -5$ делится на 5.

2) $x \equiv 2 \pmod 3$. 4) $\left.\begin{aligned} x &\equiv 3, \\ x &\equiv 4. \end{aligned}\right\} \pmod 5$ 6) $x \equiv 1 \pmod 5$.

8) Решений нет.

10) $x \equiv 4 \pmod 5$.

200. 1) Испытывая вычеты $0, \pm 1, \pm 2$, находим одно из решений $\alpha_1 \equiv -1 \equiv 4 \pmod 5$. Пишем тождественное сравнение:

$$f(x) \equiv (x - 4) f_1(x) \pmod 5. \qquad (1)$$

Находим $f_1(x)$ как частное от деления $f(x)$ на $x - 4$:

$$f_1(x) = x^2 + 8x + 32 \equiv 0 \pmod 5.$$

Это сравнение имеет решение $\alpha_2 \equiv -2 \equiv 3 \pmod 5$, следовательно,

$$f_1(x) \equiv (x - 3) f_2(x) \pmod 5. \qquad (2)$$

Находим $f_2(x)$ как частное от деления $f_1(x)$ на $x-3$:

$$f_2(x) = x + 11 \equiv 0 \pmod 5.$$

Решая это сравнение, получаем $x \equiv 4 \pmod 5$, следовательно,

$$f_2(x) \equiv x - 4 \pmod 5. \qquad (3)$$

Теперь из сравнений (1), (2), (3) окончательно имеем тождественное сравнение:

$$f(x) \equiv (x-3)(x-4)^2 \pmod 5.$$

Решение $x \equiv 4 \pmod 5$ оказалось двукратным.

Сравнение $(x-3)(x-4)^2 \equiv 0 \pmod 5$ является равносильным данному. Левая часть его, или правая часть тождественного сравнения, представляет собой разложение на множители функции $f(x) = x^3 + 4x^2 - 3$ по модулю 5.

Другая форма решения. Имеем сравнение $x^3 + 4x^2 - 3 \equiv 0 \pmod 5$, или $x^3 - x^2 + 2 \equiv 0 \pmod 5$. Его решения:

$$\left.\begin{aligned} x &\equiv -1, \\ x &\equiv -2. \end{aligned}\right\} \pmod 5$$

Пишем тождественное сравнение $f(x) \equiv (x+1)(x+2) f_1(x) \pmod 5$. Для нахождения $f_1(x)$ делим $f(x) = x^3 - x^2 + 2$ на $(x+1)(x+2)$. Получаем $f(x) = [(x+1)(x+2)](x-4) + (10x+10) \equiv (x+1) \times (x+2)(x-4) \equiv (x+1)^2(x+2) \pmod 5$, или

$$f(x) \equiv (x-3)(x-4)^2 \pmod 5.$$

3) $f(x) = (x-2)^2(x-3)(x-4) \pmod{11}$.

5) Сравнение $3x^3 - 1 \equiv 0 \pmod 5$ имеет решение $\alpha \equiv 3 \pmod 5$. Пишем тождественное сравнение $3x^3 - 1 \equiv (x-3) f_1(x) \pmod 5$. Находим $f_1(x)$ как частное от деления $3x^3 - 1$ на $x - 3$; получаем $f_1(x) = 3x^2 + 9x + 27 \equiv 0 \pmod 5$, или после упрощения

$$f_1(x) \equiv 3x^2 + 4x + 2 \equiv 0 \pmod 5.$$

Но это сравнение не имеет решений по модулю 5, поэтому окончательно получаем:

$$3x^3 - 1 \equiv (x-3)(3x^2 + 4x + 2) \pmod 5.$$

7) $f(x) \equiv (x-2)^2(x-5)^2 \pmod 7$.

9) Решений нет.

10) $f(x) \equiv (x-2)(x-3)(x^2 - 2x + 3) \pmod 7$.

201. При делении m на p имеем $m = pq + r$, по следствию из теоремы Ферма для любого x:

$$x^p \equiv x \pmod p.$$

Возведем обе части этого сравнения в степень q:

$$x^{pq} \equiv x^q \pmod p;$$

умножив на x^r, получаем:

$$x^m = x^{pq+r} \equiv x^{q+r} \pmod p. \qquad (1)$$

Теперь, если в сравнении

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod p$$

$n > p$ и $a_0 \not\equiv 0 \pmod p$, то, представляя $n = pq + r$, согласно (1) получаем

$$x^n \equiv x^{q+r} \pmod p,$$

и, умножив члены этого сравнения на a_0, будем иметь:

$$a_0x^n \equiv a_0x^{q+r} \pmod p. \qquad (2)$$

Аналогично:

$$a_1x^{n-1} \equiv a_1x^{q+r-1} \pmod p \qquad (3)$$

и т. д. Возьмем очевидное сравнение:

$$a_n \equiv a_n \pmod p. \qquad (4)$$

Теперь, складывая сравнения (2), (3), ... ,(4), будем иметь:

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv a_0x^{q+r} + a_1x^{q+r-1} + \ldots + a_n \equiv 0 \pmod p.$$

202. 1) Предварительно упростим сравнение, заменив коэффициенты их абсолютно наименьшими вычетами по модулю 13. Получаем:

$5x^{20} + 2x^{19} + 6x^{18} - 2x^{17} + 4x^{16} - 4x^{15} + 3x^6 + 4x^3 + 3x^2 - 5x - 2 \equiv 0 \pmod{13}$. Так как $20 = 13 \cdot 1 + 7$, то $q + r = 1 + 7 = 8$. Теперь имеем:

$5x^8 + 2x^7 + 6x^6 - 2x^5 + 4x^4 - 4x^3 + 3x^6 + 4x^3 + 3x^2 - 5x - 2 \equiv 0 \pmod{13}$,

или после приведения подобных членов

$5x^8 + 2x^7 - 4x^6 - 2x^5 + 4x^4 + 3x^2 - 5x - 2 \equiv 0 \pmod{13}$.

Чтобы решить это сравнение, испытываем вычеты: 0, ± 1, ± 2, ± 3, ± 4, ± 5, ± 6. Подстановкой убеждаемся, что сравнение решений не имеет, значит, не имеет решений и исходное сравнение.

2) $5x - 3 \equiv 0 \pmod 7$, его решение $x \equiv 2 \pmod 7$.

3) Решение аналогично решению задачи 202, 1). После упрощений получаем сравнение:

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

Его решения:

$$\left.\begin{aligned} x &\equiv 2, \\ x &\equiv 4. \end{aligned}\right\} \pmod{11}.$$

4) $2x^8 + 4x^5 + x + 5 \equiv 0 \pmod{11}$; его решения:

$$\left.\begin{aligned} x &\equiv 3, \\ x &\equiv 5 \end{aligned}\right\} \pmod{11}.$$

203. Из теоретического курса известно, что сравнение

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod p$$

степени $n < p$ по простому модулю p имеет n различных решений тогда и только тогда, когда остаток при делении $x^p - x$ на $f(x)$ имеет коэффициенты, кратные p. Поэтому, разделив $x^7 - x$ на $x^3 + ax + b$, получаем остаток:

$$R(x) = 2abx^2 + (b^2 - 1 - a^3)x - a^2b.$$

Чтобы сравнение $x^3 + ax + b \equiv 0 \pmod p$ имело три решения, необходимо иметь коэффициенты $R(x)$, кратные 7, что невозможно, так как, по условию, a не делится на 7 и b не делится на 7, следовательно, уже $2ab$ не делится на 7, не говоря о других коэффициентах.

204. Деля $x^p - x$ последовательно на $x^n - a$, получаем:

первый остаток $ax^{p-n} - x$,
второй остаток $a^2x^{p-2n} - x$,
третий остаток $a^3x^{p-3n} - x$,
. . . . . .
k-й остаток $a^kx^{p-kn} - x$.

Если положим, что k-й остаток является и последним, т. е. $R(x) = a^kx^{p-kn} - x$, то необходимым и достаточным условием того, чтобы сравнение $x^n \equiv a \pmod p$ имело n решений, является делимость всех коэффициентов $R(x)$ на p (см. начало решения предыдущей задачи).

Если будет $p - kn > 1$, то коэффициенты a^k и 1 являются не кратными p, и, следовательно, в этом случае сравнение не будет иметь n решений.

Если будет $p - kn = 1$, откуда $k = \dfrac{p-1}{n}$ и остаток $R(x) = (a^{\frac{p-1}{n}} - 1)x$, то, чтобы сравнение $x^n \equiv a \pmod p$ имело n решений, необходимо иметь коэффициент $a^{\frac{p-1}{n}} - 1$, кратным p, т. е. должно иметь место сравнение $a^{\frac{p-1}{n}} \equiv 1 \pmod p$ и, кроме того, необходимо, чтобы $p - 1$ делилось на n.

205. 1) Так как $1^{\frac{7-1}{3}} = 1 \equiv 1 \pmod 7$, то данное сравнение имеет три решения. Действительно, непосредственным испытанием абсолютно наименьших вычетов 0, ± 1, ± 2, ± 3 по модулю 7 находим: $x \equiv 1$, $x \equiv 2$, $x \equiv -3 \pmod 7$.

3) $10^{\frac{11-1}{5}} = 10^2 = 100 \equiv 1 \pmod{11}$; решения $x \equiv -1, 2, -4, -5 \pmod{11}$.

4) Так как 11—1 не делится на 4, то сравнение не имеет 4 решений, но имеет 2 решения: $x = \pm 2 \pmod{11}$.

206. По теореме Вильсона:

$$(p-1)! + 1 \equiv 0 \pmod p.$$

Но это сравнение можно представить так:
$(p-2)!\,(p-1) + 1 = (p-2)!\,p - (p-2)! + 1 \equiv (p-2)! - 1 \equiv 0 \pmod p$.
Можно пойти далее и получить сравнения вида:
$(p-3)!\,2 + 1 \equiv 0 \pmod p$, $(p-4)!\,6 - 1 \equiv 0 \pmod p$ и т. д.

207. По теореме Вильсона:

$$(p-1)! + 1 \equiv 0 \pmod p.$$

Умножив члены этого сравнения на 4 и сложив с очевидным сравнением $p \equiv 0 \pmod p$, получим:

$$4\,[(p-1)! + 1] + p \equiv 0 \pmod p. \qquad (1)$$

Теперь возьмем сравнение:

$$p+2 \equiv 0 \pmod{p+2}, \text{ или } p \equiv -2 \pmod{p+2}.$$

Умножим обе части этого сравнения на $p+1$;

$p(p+1)=-2(p+1)=-2[(p+2)-1]=-2(p+2)+2 \equiv 2 \pmod{p+2}$,

т. е.

$$p(p+1) \equiv 2 \pmod{p+2}.$$

Умножим обе части полученного сравнения на $(p-1)!\,2$:

$$(p-1)!\,p(p+1)\cdot 2 \equiv (p-1)!\cdot 4 \pmod{p+2},$$

или

$$(p+1)!\,2 \equiv (p-1)!\,4 \pmod{p+2}.$$

Прибавим к обеим частям по $4+p$:

$$(p+1)!\,2+2+(p+2) \equiv (p-1)!\,4+4+p \pmod{p+2},$$

или

$$2[(p+1)!+1]+(p+2) \equiv 4[(p-1)!+1]+p \pmod{p+2}. \quad (2)$$

Если $p+2$ — простое число, то по теореме Вильсона $(p+1)!+1 \equiv 0 \pmod{p+2}$, поэтому для левой части сравнения (2) имеем:

$$2[(p+1)!+1]+(p+2) \equiv 2[(p+1)!+1] \equiv 0 \pmod{p+2}. \quad (3)$$

В силу (3) и правая часть сравнения (2):

$$4[(p-1)!+1]+p \equiv 0 \pmod{p+2}. \quad (4)$$

В таком случае из (1) и (4) по третьему особому свойству сравнений имеем:

$$4[(p-1)!+1]+p \equiv 0 \pmod{p(p+2)}. \quad (5)$$

Обратно, из (5) и (1) следует (4), откуда в силу (2) получаем $(p+1)!+1 \equiv 0 \pmod{p+2}$, а это в силу теоремы Вильсона означает, что $p+2$ — простое число.

208. По теореме Вильсона:

$$(p-1)! \equiv -1 \pmod{p}.$$

Полагая $p=4n+1$, имеем:

$$(4n)! = 1\cdot 2\cdot 3\cdot \ldots \cdot 4n \equiv -1 \pmod{p}. \quad (1)$$

Возьмем часть натурального ряда:

$$(2n+1),\ (2n+2),\ \ldots,\ (4n-1),\ 4n.$$

Наименьшее число этого ряда:

$$2n+1=(4n+1)-2n=p-2n,$$

наибольшее $4n=p-1$.

Теперь $(2n+1)(2n+2)\ldots(4n-1)\,4n=(p-2n)(p-2n+1)\ldots$ $\ldots(p-2)(p-1) \equiv (-1)^{2n}\cdot 1\cdot 2\cdot 3\cdot \ldots \cdot 2n=(2n)! \pmod{p}$.

Итак,

$$(2n)! \equiv (2n+1)(2n+2)\ldots(4n-1)\,4n \pmod{p}.$$

Умножим обе части этого сравнения на $(2n)!$:

$$[(2n)!]^2 \equiv (4n)! \pmod p.$$

Теперь, учитывая (1), имеем:

$$[(2n)!]^2 \equiv -1 \pmod p.$$

§ 17. Сравнения высших степеней по составному модулю

209. 1) Сравнение $3x^3 + 4x^2 - 7x - 6 \equiv 0 \pmod{15}$ заменяем равносильной ему системой:

$$\left.\begin{aligned} 3x^3 + 4x^2 - 7x - 6 &\equiv 0 \pmod 3, \\ 3x^3 + 4x^2 - 7x - 6 &\equiv 0 \pmod 5. \end{aligned}\right\}$$

После упрощений получаем систему:

$$\left.\begin{aligned} x^2 - x &\equiv 0 \pmod 3, \\ 2x^3 + x^2 + 2x + 1 &\equiv 0 \pmod 5. \end{aligned}\right\}$$

Путем испытаний абсолютно наименьших вычетов находим решения:

$$x \equiv 0;\ 1 \pmod 3 \text{ и } x \equiv \pm 2 \pmod 5.$$

Теперь имеем четыре системы:

$$\left.\begin{aligned} x &\equiv 0 \pmod 3, \\ x &\equiv 2 \pmod 5; \end{aligned}\right\} \qquad \left.\begin{aligned} x &\equiv 0 \pmod 3, \\ x &\equiv -2 \pmod 5; \end{aligned}\right\}$$

$$\left.\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 2 \pmod 5; \end{aligned}\right\} \qquad \left.\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv -2 \pmod 5. \end{aligned}\right\}$$

решая которые, получаем четыре решения данного сравнения:

$$x \equiv -3;\ 3;\ 7;\ -2 \pmod{15}.$$

2) $-13,\ -10,\ -4,\ 2,\ 5,\ 11.$

Указание. Данное в условии сравнение заменить системой по модулям 5 и 6 или по модулям 2, 3, 5.

210. 1) Для решения сравнения $f(x) = 4x^3 - 8x - 13 \equiv 0 \pmod{27}$ рассмотрим сравнение $4x^3 - 8x - 13 \equiv 0 \pmod 3$, или после упрощения

$$x^3 - 2x - 1 \equiv 0 \pmod 3.$$

Путем испытаний абсолютно наименьших вычетов $0,\ \pm 1$ находим его решение $x \equiv 2 \pmod 3$, или

$$x = 3t_1 + 2. \tag{1}$$

Теперь составляем сравнение:

$$\frac{f(2)}{3} + f'(2)t_1 \equiv 0 \pmod 3.$$

Имеем: $f(2) = 3$, $f'(2) = 40$; $\dfrac{3}{3} + 40t_1 \equiv 0 \pmod 3$, откуда $t_1 \equiv 2 \pmod 3$, или $t_1 = 3t_2 + 2$.

Найденное значение t_1 подставляем в равенство (1):

$$x = 3(3t_2 + 2) + 2 = 9t_2 + 8. \tag{2}$$

Опять составляем сравнение:

$$\frac{f(8)}{9} f'(8)\, t_2 \equiv 0 \pmod 3.$$

Имеем: $f(8) = 1971$, $f'(8) = 760$; $\dfrac{1971}{9} + 760t_2 \equiv 0 \pmod 3$, откуда $t_2 \equiv 0 \pmod 3$, или $t_2 = 3t_3$. Это значение t_2 подставляем в равенство (2) и находим $x = 9(3t_3) + 8 = 27t_3 + 8$, или $x \equiv 8 \pmod{27}$ — искомое решение данного в условии сравнения.

3) Для решения сравнения $x^4 - 4x^3 + 2x^2 + x + 6 \equiv 0 \pmod{25}$ берем сравнение $x^4 - 4x^3 + 2x^2 + x + 6 \equiv 0 \pmod 5$, упростив которое, получаем $x^4 + x^3 + 2x^2 + x + 1 \equiv 0 \pmod 5$. Путем испытаний абсолютно наименьших вычетов $0, \pm 1, \pm 2$ находим его решение:

$$x_1 \equiv 2 \pmod 5, \text{ или } x_1 = 5t_1 + 2,$$
$$x_2 \equiv -2 \pmod 5, \text{ или } x_2 = 5t_1 - 2.$$

Теперь для первого решения имеем:

$$\frac{f(2)}{5} + f'(2)t_1 \equiv 0 \pmod 5, \quad \frac{0}{5} - 7t_1 \equiv 0 \pmod 5,$$

откуда $t_1 \equiv 0 \pmod 5$, или $t_1 = 5t_2$, поэтому

$$x_1 = 5(5t_2) + 2 = 25t_2 + 2, \text{ или } x_1 \equiv 2 \pmod{25}.$$

Для второго решения получаем:

$$\frac{f(-2)}{5} + f'(-2)\,t_1 \equiv 0 \pmod 5, \quad \frac{60}{5} - 87t_1 \equiv 0 \pmod 5,$$

откуда $t_1 \equiv 1 \pmod 5$, или $t_1 = 5t_2 + 1$, и потому

$$x_2 = 5(5t_2 + 1) - 2 = 25t_2 + 3, \text{ или } x_2 \equiv 3 \pmod{25}.$$

5) Для решения сравнения $6x^3 - 7x - 11 \equiv 0 \pmod{125}$ берем сравнение $6x^3 - 7x - 11 \equiv 0 \pmod 5$, упростив которое, получаем:

$$x^3 - 2x - 1 \equiv 0 \pmod 5.$$

Его решения:

$$x_1 \equiv -1 \pmod 5, \text{ или } x_1 = 5t_1 - 1,$$
$$x_2 \equiv -2 \pmod 5, \text{ или } x_2 = 5t_1 - 2.$$

Дальше находим первое решение для данного сравнения:

$$x_1 \equiv -41 \pmod{125}.$$

Для второго решения имеем: $f(-2) = -45$, $f'(-2) = 65$. Как видим, $f'(-2) = 65$ делится на 5, следовательно, сравнение

$$\frac{f(-2)}{5} + f'(-2)\,t_1 \equiv 0 \pmod 5$$

неразрешимо относительно t_1; это значит, что данное сравнение второго решения не имеет.

211. 1) Решение сравнения $x^4 - x^3 + 2x^2 + x + 12 \equiv 0 \pmod{45}$ сводится к решению системы:

$$\left.\begin{aligned} x^4 - x^3 + 2x^2 + x + 2 &\equiv 0 \pmod 5, \\ x^4 + 4x^3 + 2x^2 + x + 3 &\equiv 0 \pmod 9. \end{aligned}\right\}$$

Первое сравнение системы имеет решения:

$$x \equiv \pm 1 \pmod 5 \text{ и } x \equiv 2 \pmod 5.$$

Для решения второго сравнения берем сравнение $x^4 + x^3 + 2x^2 + x \equiv 0 \pmod 3$, которое имеет решение $x \equiv 0 \pmod 3$, или $x = 3t_1$; t_1 находим из сравнения

$$\frac{f(0)}{3} + f'(0)t_1 \equiv 0 \pmod 3,$$

где $f(x) = x^4 + 4x^3 + 2x^2 + x + 3$:

$$\frac{3}{3} + 1 \cdot t_1 \equiv 0 \pmod 3, \text{ откуда } t_1 \equiv -1 \pmod 3, \text{ или } t_1 = 3t_2 - 1.$$

Получаем:

$x = 3t_1 = 3(3t_2 - 1) = 9t_2 - 3$, или $x \equiv -3 \pmod 9$ — решение второго сравнения системы.

Теперь для решения сравнения, данного в условии, имеем системы:

$$\left.\begin{array}{l} x \equiv 1 \pmod 5, \\ x \equiv -3 \pmod 9; \end{array}\right\} \quad \left.\begin{array}{l} x \equiv -1 \pmod 5, \\ x \equiv -3 \pmod 9; \end{array}\right\} \quad \left.\begin{array}{l} x \equiv 2 \pmod 5, \\ x \equiv -3 \pmod 9, \end{array}\right\}$$

решая которые, находим:

$$x \equiv 6 \pmod{45}; \quad x \equiv 24 \pmod{45}; \quad x \equiv 42 \pmod{45}.$$

2) 12, 24, 37, 49.

6) Сравнение $4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{9 \cdot 25}$ заменяем системой,

$$\left.\begin{array}{l} 4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod 9, \\ 4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{25}, \end{array}\right\}$$

или

$$\left.\begin{array}{l} 4x^3 - 2x^2 + 2x - 1 \equiv 0 \pmod 9, \\ 4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{25}. \end{array}\right\}$$

Применяя принятый нами способ, получаем решения: для первого сравнения $x \equiv 7 \pmod 9$, для второго сравнения $x \equiv -5 \pmod{25}$, $x \equiv -1 \pmod{25}$, $x \equiv -2 \pmod{25}$. Получаем системы:

$$\left.\begin{array}{l} x \equiv 7 \pmod 9, \\ x \equiv -5 \pmod{25}; \end{array}\right\} \quad \left.\begin{array}{l} x \equiv 7 \pmod 9, \\ x \equiv -1 \pmod{25}; \end{array}\right\} \quad \left.\begin{array}{l} x \equiv 7 \pmod 9, \\ x \equiv -2 \pmod{25}. \end{array}\right\}$$

Решая их, находим $x \equiv 70;\ 124;\ 223 \pmod{9 \cdot 25}$.

§ 18. Сравнения второй степени. Символ Лежандра

212. Испытывая числа 1, 2, 3,..., 10 с помощью критерия Эйлера $a^{\frac{p-1}{2}} = a^5 \equiv \pm 1 \pmod{11}$, имеем:

$$\left.\begin{array}{l} 1^5 \equiv 1, \\ 2^5 = 32 \equiv -1, \\ 3^5 = 243 \equiv 1, \\ 4^5 = 16^2 \cdot 4 = 256 \cdot 4 \equiv 3 \cdot 4 \equiv 1, \\ 5^5 = 5^3 \cdot 5^2 = 125 \cdot 25 \equiv 4 \cdot 3 \equiv 1, \\ 6^5 = (6^2)^2 \cdot 6 = 36^2 \cdot 6 \equiv 3^2 \cdot 6 = 54 \equiv -1, \\ 7^5 = (7^2)^2 \cdot 7 = 49^2 \cdot 7 \equiv 5^2 \cdot 7 = 3 \cdot 7 \equiv -1, \\ 8^5 = (8^2)^2 \cdot 8 = 64^2 \cdot 8 \equiv (-2)^2 \cdot 8 = 32 \equiv -1, \\ 9^5 = (9^2)^2 \cdot 9 = 81^2 \cdot 9 \equiv 4^2 \cdot 9 = 16 \cdot 9 \equiv 5 \cdot 9 \equiv 1, \\ 10^5 \equiv (-1)^5 = -1. \end{array}\right\} \pmod{11}$$

Итак, числа 1, 3, 4, 5, 9 — квадратичные вычеты по модулю 11.

213. 1) Испытывая числа 1, 2, 3, 4, 5, 6 с помощью критерия Эйлера $a^{\frac{p-1}{2}} = a^3 \equiv \pm 1 \pmod 7$, получаем:

$$\left.\begin{aligned} &1^3 \equiv 1,\\ &2^3 \equiv 1,\\ &3^3 = 27 \equiv -1,\\ &4^3 = 64 \equiv 1,\\ &5^3 \equiv (-2)^3 = -8 \equiv -1,\\ &6^3 \equiv (-1)^3 = -1. \end{aligned}\right\} \pmod 7$$

Итак, квадратичными вычетами являются числа 1, 2, 4 или классы чисел по модулю 7:

$$7k + 1,\quad 7k + 2,\quad 7k + 4.$$

214. 1) Испытывая вычеты ± 1, ± 2, ± 3, находим:

$$x \equiv \pm 3 \pmod 7.$$

2) $x \equiv \pm 2 \pmod 7$.

3) Неразрешимо.

215. 1) Пользуясь законом взаимности, имеем:

$$\left(\frac{63}{131}\right) = \left(\frac{3}{131}\right)^2 \left(\frac{7}{131}\right) = \left(\frac{7}{131}\right) = (-1)^{3\cdot 65}\left(\frac{131}{7}\right) = (-1)\left(\frac{5}{7}\right) =$$

$$= (-1)(-1)^{2\cdot 3}\left(\frac{7}{5}\right) = (-1)\left(\frac{2}{5}\right) = (-1)(-1)^{\frac{25-1}{8}} = (-1)(-1)^3 = 1.$$

3) $\left(\frac{47}{73}\right) = (-1)^{23\cdot 36}\left(\frac{73}{47}\right) = \left(\frac{26}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{13}{47}\right) =$

$$= (-1)^{\frac{47^2-1}{8}} \cdot (-1)^{6\cdot 23}\left(\frac{47}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{2}{13}\right)^2 \cdot \left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}}$$

$$= -1.$$

5) -1. 7) 1.

216. Находим символ Лежандра:

$$\left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = (-1)^{\frac{7^2-1}{8}}(-1)^{1\cdot 3}\left(\frac{7}{3}\right) = (-1)\left(\frac{1}{3}\right) = -1,$$

следовательно, сравнение неразрешимо.

3) $\left(\frac{12}{13}\right) = 1$, решения $x \equiv \pm 15 \pmod{13}$. 5) $\left(\frac{5}{11}\right) = 1$, решения $x \equiv \pm 4 \pmod{11}$.

217. 1) Умножив члены сравнения на 12, получим:

$$36x^2 + 12 \cdot 7x + 96 \equiv 0 \pmod{17}, \text{ или } (6x + 7)^2 \equiv 4 \pmod{17},$$

$$y^2 \equiv 4 \pmod{17}, \text{ где } y = 6x + 7.$$

Сравнение $y^2 \equiv 4 \pmod{17}$ имеет решения $y \equiv \pm 2 \pmod{17}$. Теперь для решения исходного сравнения надо решить сравнения:

$$\left.\begin{array}{l} 6x + 7 \equiv 2, \\ 6x + 7 \equiv -2, \end{array}\right\} \pmod{17},$$

решая которые, получаем:

$$\left.\begin{array}{l} x \equiv 2, \\ x \equiv 7. \end{array}\right\} \pmod{17}$$

Проверкой убеждаемся, что полученные решения удовлетворяют данному в условии сравнению.

3) Неразрешимо. 5) $x \equiv 2, \ 3 \pmod{13}$.

218. По критерию Эйлера, если a — квадратичный вычет, то $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Умножив обе части этого сравнения на a, получим:

$$a^{\frac{p+1}{2}} \equiv a \pmod{p}.$$

Заменяя в левой части p через $4k + 3$, будем иметь:

$$a^{2k+2} \equiv a \pmod{p},$$

или

$$(a^{k+2})^2 \equiv a \pmod{p},$$

откуда $x \equiv \pm a^{k+1} \pmod{p}$.

219. 1) Число 2 есть квадратичный вычет по модулю 311, так как

$$\left(\frac{2}{311}\right) = (-1)^{\frac{311^2-1}{8}} = (-1)^{\frac{310 \cdot 312}{8}} = (-1)^{310 \cdot 39} = 1.$$

Имеем: $p = 311 = 77 \cdot 4 + 3$, $k = 77$.

Поэтому

$$x \equiv \pm 2^{k+1} = \pm 2^{78} = (\pm 1)\ (2^{12})^6 \cdot 2^6 = (\pm 1)\ 4096^6 \cdot 2^6 \equiv$$
$$\equiv (\pm 1) \cdot (53 \cdot 2)^6 = (\pm 1)\ (106^2)^3 = (\pm 1)\ 11\,236^3 \equiv (\pm 1)\ 40^3 =$$
$$= (\pm 1).\ 64\,000 \equiv (\pm 1)\ (-66) = \pm 66 \pmod{311}.$$

2) $x \equiv \pm 12 \pmod{47}$.

220. Если $p = 8k + 5$, то $\frac{p-1}{2} = 4k + 2$ и по критерию Эйлера

$$a^{\frac{p-1}{2}} = a^{4k+2} \equiv 1 \pmod{p},$$

или

$$(a^{2k+1} - 1)(a^{2k+1} + 1) \equiv 0 \pmod{p}.$$

Отсюда либо $p / a^{2k+1} - 1$, либо $p / a^{2k+1} + 1$, так как оба сомножителя одновременно не могут делиться на p, ибо их разность не делится на p. Итак, должен иметь место один из двух случаев:

1) $a^{2k+1} \equiv 1 \pmod{p}$, $(a^{k+1})^2 \equiv a \pmod{p}$,

$x \equiv \pm a^{k+1} \pmod{p}$ — решение данного сравнения;

2) $a^{2k+1} \equiv -1 \pmod{p}$, $(a^{k+1})^2 \equiv -a \pmod{p}$.

Возьмем какой-либо квадратичный невычет по модулю $p = 8k + 5$.

Наименьшим будет число 2, так как

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8k+5)^2-1}{8}} = (-1)^{(2k+1)(4k+3)} = -1.$$

По критерию Эйлера

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

заменяя p в левой части числом $8k+5$, получим:

$$2^{4k+2} \equiv -1 \pmod{p}.$$

Умножаем это сравнение на сравнение, полученное во втором случае:

$$(a^{k+1})^2 \cdot 2^{4k+2} \equiv (-a)(-1) \pmod{p},$$

или

$$(a^{k+1} \cdot 2^{2k+1})^2 \equiv a \pmod{p},$$

откуда следует решение:

$$x \equiv \pm a^{k+1} \cdot 2^{2k+1} \pmod{p}.$$

Объединяя это решение с полученным в первом случае, окончательно имеем:

$$x \equiv \pm a^{k+1} \cdot 2^{(2k+1)t} \pmod{p}, \text{ где } t = 0 \text{ или } t = 1,$$

причем $t = 0$ в случае, когда

$$a^{2k+1} \equiv 1 \pmod{p},$$

и $t = 1$ в случае, когда

$$a^{2k+1} \equiv -1 \pmod{p}.$$

221. 1) $p = 29 = 8 \cdot 3 + 5$, $k+1 = 4$, $2k+1 = 7$; число $a = 7$ — квадратичный вычет, так как

$$\left(\frac{7}{29}\right) = (-1)^{3 \cdot 14}\left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

Поскольку $a^{2k+1} = 7^7 = (7^2)^3 \cdot 7 \equiv 20^3 \cdot 7 = 56\,000 \equiv 1 \pmod{29}$, то берем $t = 0$ и получаем:

$$x \equiv \pm 7^{k+1} = (\pm 1)\ 7^4 = (\pm 1)\ 49^2 \equiv (\pm 1)\ 20^2 \equiv (\pm 1)(-6) \equiv \equiv \pm 6 \pmod{29}.$$

2) $p = 37 = 8 \cdot 4 + 5$, $k+1 = 5$, $2k+1 = 9$; число $a = 3$ — квадратичный вычет, так как $\left(\frac{3}{37}\right) = (-1)^{1 \cdot 18}\left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1$.

Поскольку $a^{2k+1} = 3^9 = (3^4)^2 \cdot 3 \equiv 7^2 \cdot 3 \equiv 12 \cdot 3 \equiv -1 \pmod{37}$, то берем $t = 1$ и получаем:

$$x \equiv \pm 3^5 \cdot 2^9 = (\pm 1)\,243 \cdot 512 \equiv (\pm 1) \cdot 21 \cdot (-6) = (\pm 1)(-126) \equiv \equiv (\pm 1)(-15) \equiv \pm 15 \pmod{37}.$$

222. Указание. Надо рассмотреть сравнение $5x^2 - 7 \equiv \equiv 0 \pmod{11}$.

223. Указание. Надо доказать, что $x(x+1) \not\equiv 1 \pmod{13}$.

224. Рассмотрим сравнение:

$$x^2 - 21x + 110 \equiv 0 \pmod{13},$$

или

$$x^2 - 8x + 6 = 0 \pmod{13}.$$

Теперь

$$(x - 4)^2 \equiv 36 \pmod{13},$$

откуда

$$x_1 = 10 + 13t,$$
$$x_2 = 11 + 13t.$$

Поэтому

$$y_1 = 13t^2 - t, \quad y_2 = 13t^2 + t.$$

Заменяя в x_2, y_2 величину t через $-t$, получаем: если $x = 10 + 13t$, или $x = 11 - 13t$, то $y = 13t^2 - t$.

225. Ответ. $x \equiv 1, 57, 79, 122 \pmod{143}$.

226. 2 — квадратичный вычет по модулю $p = 8k + 7$. Действительно, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{(8k+6)(k+1)} = 1$. В таком случае $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$; аналогично убеждаемся, что по модулю $p = 8k + 3$ число 2 — квадратичный невычет.

227. Если a — квадратичный вычет по модулю $p = 4k + 3$, то по критерию Эйлера

$$a^{\frac{p-1}{2}} = a^{2k+1} \equiv 1 \pmod{p}.$$

Беря вместо a число $-a$, получаем:

$$a^{2k+1} \equiv -1 \pmod{p}$$

и $-a$ — квадратичный невычет.

Аналогично решается и вторая часть задачи.

228. Имеем по закону квадратичной взаимности:

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

Таким образом, величина символа Лежандра $\left(\frac{3}{p}\right)$ зависит от $\left(-1\right)^{\frac{p-1}{2}}$ и от $\left(\frac{p}{3}\right)$.

Если $\frac{p-1}{2} = 2n-1$, $p = 4n-1$, $p \equiv -1 \pmod{4}$, то

$$(-1)^{\frac{p-1}{2}} = -1. \tag{1}$$

Если $\frac{p-1}{2} = 2n$, $p = 4n+1$, $p \equiv 1 \pmod{4}$, то

$$(-1)^{\frac{p-1}{2}} = 1. \qquad (2)$$

Величина $\left(\frac{p}{3}\right)$ может иметь два значения. Если $p \equiv 1 \pmod 3$, то

$$\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1. \qquad (3)$$

Если $p \equiv 2 \equiv -1 \pmod 3$, то

$$\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1. \qquad (4)$$

Теперь видим, что 3 будет квадратичным вычетом, если одновременно будут иметь место (1) и (4) или (2) и (3). В первом случае $p \equiv -1 \pmod 4$ и $p \equiv -1 \pmod 3$, что дает $p \equiv -1 \pmod{12}$, $p \equiv 12k - 1$. Во втором случае $p \equiv 1 \pmod 4$ и $p \equiv 1 \pmod 3$, откуда $p \equiv 1 \pmod{12}$, $p = 12k + 1$.

3 будет квадратичным невычетом, если одновременно имеют место условия (1) и (3) или (2) и (4). В первом случае $p \equiv -1 \pmod 4$, $p \equiv 1 \pmod 3$. Решая эту систему, находим $p = 12k - 5$. Во втором случае находим $p = 12k + 5$.

Итак, если $p = 12k \pm 1$, то 3 — квадратичный вычет, если же $p = 12k \pm 5$, то 3 — квадратичный невычет.

§ 19. Числа, принадлежащие показателю; первообразные корни

229. 1) Испытывая числа 2, 3, 4, взаимно простые с 5, с показателями 1, 2, 4 — делителями $\varphi(5) = 4$, имеем:

$2^1 \not\equiv 1$, $2^2 \not\equiv 1$, $2^4 \equiv 1$, следовательно, число 2 принадлежит показателю $\delta = 4$ по модулю 5;

$3^1 \not\equiv 1$, $3^2 \not\equiv 1$, $3^4 \equiv 1$, следовательно, число 3 принадлежит показателю $\delta = 4$ по модулю 5;

$4^1 \not\equiv 1$, $4^2 \equiv 1$, следовательно, число 4 принадлежит показателю $\delta = 2$ по модулю 5.

Числа 2 и 3 являются первообразными корнями по модулю 5.

3) Испытывая числа 3, 5, 7, взаимно простые с 8, с показателями 1, 2, 4 — делителями $\varphi(8) = 4$, получаем:

$3^1 \not\equiv 1$, $3^2 \equiv 1$, следовательно, число 3 принадлежит показателю $\delta = 2$ по модулю 8;

$5^1 \not\equiv 1$, $5^2 \equiv 1$, следовательно, число 5 принадлежит показателю $\delta = 2$ по модулю 8;

$7^1 \not\equiv 1$, $7^2 \equiv 1$, следовательно, число 7 принадлежит показателю $\delta = 2$ по модулю 8.

Первообразных корней по модулю 8 нет.

5) 2, 6, 7, 8 принадлежат показателю $\delta = 10$ по модулю 11.

3, 4, 5, 9 принадлежат показателю $\delta = 5$ по модулю 11.

10 принадлежит показателю $\delta = 2$ по модулю 11.

230. 1) Имеем: $p = 11$, $\varphi(11) = 10$, $d_1 = 2$, $d_2 = 5$, сравнения для испытаний:

$$g^5 \not\equiv 1 \pmod{11}, \quad g^2 \not\equiv 1 \pmod{11}.$$

Испытываем числа 2, 3, 4, 5, 6, 7, 8, 9, 10, взаимно простые с 11, кроме 1, так как всегда $1^k \equiv 1$ по любому модулю $m > 1$ при всяком целом неотрицательном k. Имеем:

$$\left.\begin{array}{l} 2^5 \not\equiv 1,\ 2^2 \not\equiv 1 \\ 3^5 \equiv 1 \\ 4^5 \equiv 1 \\ 5^5 \equiv 1 \\ 6^5 \not\equiv 1,\ 6^2 \not\equiv 1 \\ 7^5 \not\equiv 1,\ 7^2 \not\equiv 1 \\ 8^5 \not\equiv 1,\ 8^2 \not\equiv 1 \\ 9^5 \equiv 1 \\ 10^5 \not\equiv 1,\ 10^2 \equiv 1 \end{array}\right\} \pmod{11}$$

Итак, первообразными корнями по модулю 11 являются числа 2, 6, 7, 8; число их $\varphi(p-1) = \varphi(10) = 4$.

3) 2, 6, 7, 11 — первообразные корни, число их $\varphi(12) = 4$.

231. 1) Имеем: $p = 19$, $\varphi(p) = 18$, $d_1 = 2$, $d_2 = 3$, формулы для испытаний $g^9 \not\equiv 1$, $g^6 \not\equiv 1 \pmod{19}$; $2^9 \not\equiv 1$, $2^6 \not\equiv 1 \pmod{19}$, следовательно, 2 — наименьший первообразный корень. Число всех корней по модулю 19 равно $\varphi(18) = 6$.

3) 8, $g = 3$. 5) 12, $g = 2$.

232. 1) Из первого примера предыдущей задачи известно, что наименьший первообразный корень по модулю 19 равен 2. Выписываем значения k=5, 7, 11, 13, 17, взаимно простые с 18. Имеем:

$$\left.\begin{array}{l} 2^5 = 32 \equiv 13 \\ 2^7 = 2^5 \cdot 2^2 \equiv 13 \cdot 4 = 52 \equiv 14 \\ 2^{11} = (2^5)^2 \cdot 2 \equiv 13^2 \cdot 2 \equiv 17 \cdot 2 \equiv 15 \pmod{19} \\ 2^{13} = 2^{11} \cdot 4 \equiv 15 \cdot 4 = 40 \equiv 3 \\ 2^{17} = 2^{10} \cdot 2^7 \equiv 17 \cdot 14 = 238 \equiv 10 \end{array}\right\}$$

Итак, числа 2, 3, 10, 13, 14, 15 — первообразные корни по модулю 19.

233. Пусть число $2^{2^n}+1$ имеет простой делитель p, тогда $2^{2^n}+1 \equiv 0 \pmod{p}$, или $2^{2^n} \equiv -1 \pmod{p}$. Возводя члены сравнения в квадрат, получим:

$$2^{2^{n+1}} \equiv 1 \pmod{p}, \qquad (1)$$

откуда видно, что основание 2 принадлежит показателю 2^{n+1} по модулю p; тогда по следствию из свойства $p-1$ делится на 2^{n+1}, или

$$p \equiv 1 \pmod{2^{n+1}}. \qquad (2)$$

Последнее сравнение справедливо при всех $n > 1$, во всяком случае, $p-1$ делится на 2^3, т. е. $p = 8t+1$.

Требование (2) можно еще больше усилить. По критерию Эйлера о квадратичных вычетах:

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

но

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8t+1)^2-1}{8}} = 1,$$

значит,

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}; \qquad (3)$$

так как в силу (1) число 2 принадлежит показателю $\delta = 2^{n+1}$, то из (3) следует:

$\frac{p-1}{2}$ делится на 2^{n+1}, откуда $p = k \cdot 2^{n+2} + 1$.

Например, при $n = 5$ имеем:

$$2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,297.$$

Возможные простые делители этого числа будут иметь вид $p = k \cdot 2^7 + 1 = 128k + 1$. Так, при $k = 5$ простое число $p = 128 \cdot 5 + 1 = 641$ есть делитель $2^{2^5} + 1$.

ГЛАВА IV

ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

§ 20. Индексы и их применение

234. 1) Находим наименьшие положительные вычеты степеней $2^0, 2^1, 2^2, \ldots, 2^{p-2}$ по модулю $p = 29$:

$2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16$, $2^5 \equiv 3$, $2^6 \equiv 6$,
$2^7 \equiv 12$, $2^8 \equiv 24$, $2^9 \equiv 19$, $2^{10} \equiv 9$, $2^{11} \equiv 18$,
$2^{12} \equiv 7$, $2^{13} \equiv 14$, $2^{14} \equiv 28$, $2^{15} \equiv 27$ $2^{16} \equiv 25$,
$2^{17} \equiv 21$, $2^{18} \equiv 13$, $2^{19} \equiv 26$, $2^{20} \equiv 23$, $2^{21} \equiv 17$, $2^{22} \equiv 5$,
$2^{23} \equiv 10$, $2^{24} \equiv 20$, $2^{25} \equiv 11$, $2^{26} \equiv 22$, $2^{27} \equiv 15$.

Составляем таблицы индексов и антииндексов:

№	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

t	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Примеры:

$\operatorname{ind} 5 = 22$, $\operatorname{ind} 10 = 23$, $\operatorname{ind} N = 5$, $N = 3$, $\operatorname{ind} N = 10$, $N = 9$,
$\operatorname{ind} 15 = 27$, $\operatorname{ind} 23 = 20$. $\operatorname{ind} N = 15$, $N = 27$, $\operatorname{ind} N = 23$, $N = 10$.

235. 1) Индексируя левую и правую части сравнения, получаем $\delta \operatorname{ind} 5 \equiv 0 \pmod 6$. По таблице индексов находим $\operatorname{ind} 5 = 5$, подставляем в сравнение: $\delta \cdot 5 \equiv \pmod 6$. Сокращая члены сравнения на 5, имеем:

$$\delta \equiv 0 \pmod 6,$$

откуда наименьшее значение $\delta = 6$.

3) $\delta = 4$, 5) $\delta = 30$, 7) $\delta = 16$.

236. 1) Выписываем числа 2, 3, 4. Индексированием решаем сравнения $2^\delta \equiv 1 \pmod 5$, $3^\delta \equiv 1 \pmod 5$, $4^\delta \equiv 1 \pmod 5$.

Имеем: $\delta \operatorname{ind} 2 \equiv 0 \pmod 4$, $\delta \operatorname{ind} 3 \equiv 0 \pmod 4$, $\delta \operatorname{ind} 4 \equiv 0 \pmod 4$; по таблице индексов находим:

$$\delta \cdot 1 \equiv 0 \pmod 4, \qquad \delta \cdot 3 \equiv 0 \pmod 4, \qquad \delta \cdot 2 \equiv 0 \pmod 4.$$

Упрощаем сравнения:

$$\delta \equiv 0 \pmod 4, \qquad \delta \equiv 0 \pmod 4, \qquad \delta \equiv 0 \pmod 2,$$

отсюда

$$\delta = 4, \qquad \delta = 4, \qquad \delta = 2.$$

Следовательно, числа 2 и 3 принадлежат показателю $\delta = 4$, а число 4 — показателю 2 по модулю 5.

237. 1) Находим индексированием показатель δ, которому принадлежит число 2 по модулю 59:

$$2^\delta \equiv 1 \pmod{59}, \quad \delta \operatorname{ind} 2 \equiv 0 \pmod{58}, \quad \delta \cdot 1 \equiv 0 \pmod{58},$$

отсюда $\delta = 58 = p-1$, следовательно, число 2 является первообразным корнем по модулю 59.

3) Число 6 — первообразный корень по модулю 59.

5) Число 12 не является первообразным корнем по модулю 59.

7) Число 14 — первообразный корень по модулю 59.

238. 1) Выписываем числа 2, 3, 4, ..., 16.

Из таблицы индексов по модулю 17 видно, что для подстановки в сравнение $\delta \operatorname{ind} a \equiv 0 \pmod{16}$ взаимно простыми с 16 являются только индексы следующих чисел: 3, 5, 6 , 7, 10, 11, 12, 14. Следовательно, эти числа принадлежат показателю $p - 1 = 16$ и являются первообразными корнями; остальные же числа 2, 4, 8, 9, 13, 15, 16 принадлежат меньшим показателям, а потому не являются первообразными корнями.

239. 1) Индексируя члены сравнения, получаем:

$x \operatorname{ind} 2 \equiv \operatorname{ind} 7 \pmod{66}$, $\quad x \cdot 1 \equiv 23 \pmod{66}$,

$x \equiv 23 \pmod{66}$, или $x = 66k + 23$ при $k = 0, 1, 2, \ldots$.

3) $x \operatorname{ind} 16 \equiv \operatorname{ind} 11 \pmod{52}$, $x \cdot 4 \equiv 6 \pmod{52}$; сокращаем члены сравнения и модуль на 2:

$$2x \equiv 3 \pmod{26}.$$

Так как $(2,26) = 2$, но 3 не делится на 2, то это сравнение не имеет решений, значит, не имеет решений и исходное сравнение.

5) $x \equiv 13 \pmod{30}$.

240. 1) Индексируя сравнение, имеем:

$$\begin{aligned}&\operatorname{ind} 7+\operatorname{ind} x\equiv \operatorname{ind} 6 \pmod{16},\\ &\operatorname{ind} x\equiv \operatorname{ind} 6-\operatorname{ind} 7 \pmod{16},\\ &\operatorname{ind} x\equiv 15-11 \pmod{16},\\ &\operatorname{ind} x\equiv 4 \pmod{16}.\end{aligned}$$

По таблице антииндексов находим $x \equiv 13 \pmod{17}$.

Проверка. $7 \cdot 13 - 23 = 91 - 23 = 68$ делится на 17.

3) $x \equiv 74 \pmod{79}$. 6) $x \equiv 30 \pmod{221}$.

Указание. Так как $221 = 13 \cdot 17$, то данное сравнение заменить системой:

$$\left.\begin{aligned}&37x\equiv 5 \pmod{13},\\ &37x\equiv 5 \pmod{17}.\end{aligned}\right\}$$

241. 1) Индексируя сравнение, получаем:

$$15 \operatorname{ind} x \equiv \operatorname{ind} 62 - \operatorname{ind} 37 = 19 - 64 \equiv 27 \pmod{72}.$$

Это сравнение первой степени относительно $\operatorname{ind} x$; так как $(15, 27, 72)=3$, то сравнение, если разрешимо, имеет три решения относительно $\operatorname{ind} x$. После сокращения имеем сравнение (разрешимое):

$$5 \operatorname{ind} x \equiv 9 \pmod{24}.$$

Решая, например, способом непрерывных дробей, получаем:

$$\operatorname{ind} x \equiv 21 \pmod{24}.$$

Поэтому:

$$\left.\begin{aligned}&\operatorname{ind} x\equiv 24\cdot 0+21\equiv 21\\ &\operatorname{ind} x\equiv 24\cdot 1+21\equiv 45\\ &\operatorname{ind} x\equiv 24\cdot 2+21\equiv 69\end{aligned}\right\} \pmod{72}.$$

По таблице антииндексов находим:

$$\left.\begin{aligned}&x\equiv 17\\ &x\equiv 63\\ &x\equiv 66\end{aligned}\right\} \pmod{73}.$$

Проверка производится подстановкой корней в сравнение, данное в условии.

3) $x \equiv 2, 3, 10, 11 \pmod{13}$.

5) После индексирования и упрощения получаем сравнение

$$5 \operatorname{ind} x \equiv 7 \pmod{30};$$

так как $(5,30) = 5$, но 7 не делится на 5, то это сравнение не имеет решений, следовательно, и исходное сравнение не имеет решений.

7) $x \equiv 13, 29, 31 \pmod{73}$. 9) $x \equiv 25, 30, 31, 36 \pmod{61}$.

242. 1) Индексируя сравнение, получаем:

$$\begin{aligned}&12 \operatorname{ind} x \equiv \operatorname{ind} 37 \pmod{40}.\\ &12 \operatorname{ind} x \equiv 32 \pmod{40}, \qquad d = (12, 32, 40) = 4,\\ &3 \operatorname{ind} x \equiv 8 \pmod{10}.\end{aligned}$$

Решение. $\operatorname{ind} x \equiv 6 \pmod{10}$. Поэтому:

$$\left.\begin{aligned}&\operatorname{ind} x\equiv 10\cdot 0+6\equiv 6\\ &\operatorname{ind} x\equiv 10\cdot 1+6\equiv 16\\ &\operatorname{ind} x\equiv 10\cdot 2+6=26\\ &\operatorname{ind} x\equiv 10\cdot 3+6=36\end{aligned}\right\} \pmod{40},$$

откуда

$$\left.\begin{array}{l} x \equiv 39 \\ x \equiv 18 \\ x \equiv 2 \\ x \equiv 23 \end{array}\right\} \pmod{41}.$$

Проверка. $2^{12} = (2^6)^2 = 64^2 \equiv 23^2 = 529 \equiv 37$; $37 \equiv 37 \pmod{41}$ и т. д. для остальных корней.

3) $x \equiv 33 \pmod{67}$.

5) Неразрешимо.

7) $x \equiv 34, 32, 20 \pmod{43}$.

9) $x \equiv \pm 27 \pmod{67}$.

11) Неразрешимо.

13) $x \equiv \pm 21 \pmod{67}$.

243. 1) Критерий Эйлера для модуля 23 будет

$$a^{11} \equiv 1 \pmod{23};$$

индексируя, получаем:

$$11 \operatorname{ind} a \equiv 0 \pmod{22}, \quad \text{или} \quad \operatorname{ind} a \equiv 0 \pmod{2}.$$

Отсюда видим, что $\operatorname{ind} a$ должен быть числом четным.
В таблице индексов по модулю 23 из заданных в условии чисел 15, 16,..., 20 имеют четные индексы только числа 16 и 18, которые, следовательно, и являются квадратичными вычетами по модулю 23.

3) Числа 16, 18, 20 — квадратичные вычеты по модулю 41.

5) Числа 16, 18 — квадратичные вычеты по модулю 97.

§ 21. Другие приложения теории сравнений

244. 1) Пишем сравнение:

$$10^{\delta} \equiv 1 \pmod{19};$$

индексируя его, находим:

$$\delta \operatorname{ind} 10 \equiv 0 \pmod{18}, \qquad \delta \cdot 17 \equiv 0 \pmod{18},$$
$$\delta \equiv 0 \pmod{18}, \qquad \delta = 18.$$

Следовательно, число цифр в периоде равно 18.

Замечание. Если число 10 является первообразным корнем по модулю p, то при обращении дроби $\frac{1}{p}$ в десятичную в периоде будет $p-1$ цифр, так как в этом случае 10 как первообразный корень принадлежит показателю $\delta = p - 1$.

3) Пишем сравнения:

$$10^{\delta} \equiv 1 \pmod{13},$$
$$10^{\delta} \equiv 1 \pmod{37};$$

индексируя их, находим:

$$\delta \operatorname{ind} 10 \equiv 0 \pmod{12}, \qquad \delta \cdot 10 \equiv 0 \pmod{12},$$
$$\delta \cdot 5 \equiv 0 \pmod{6}. \qquad \delta = 6,$$

$$\delta \operatorname{ind} 10 \equiv 0 \pmod{36}, \qquad \delta \cdot 24 \equiv 0 \pmod{36},$$
$$\delta \cdot 2 \equiv 0 \pmod{3}, \qquad \delta_1 = 3.$$

Наименьшее кратное $[6, 6_1] = [6; 3] = 6$,

Следовательно, число цифр в периоде равно 6.

5) 330 цифр. 7) 18 цифр . 9) 28 цифр.

245. Представим число N, взятое в десятичной системе счисления, так:

$$N = n_1 10^m + n_2 = n_1 10^m \pm n_1 + n_2 \mp n_1 = n_1 (10^m \pm 1) + (n_2 \mp n_1),$$

где n_2 — число, образуемое первыми m цифрами числа N, n_1 — число, образуемое оставшимися цифрами числа N.

Из полученного равенства имеем сравнение:

$$N \equiv n_2 \mp n_1 \pmod{10^m \pm 1},$$

из которого следует: чтобы число N делилось на числа вида $10^m \pm 1$ и их делители, достаточно, чтобы $n_2 \mp n_1$ делилось соответственно на $10^m \pm 1$ и их делители.

При $m = 3$ будет $10^3 + 1 = 1001 = 7 \cdot 11 \cdot 13$, получаем общий признак делимости на 7, 11, 13: чтобы число N делилось на 7, 11 или 13, достаточно, чтобы разность между числом, образуемым первыми тремя цифрами числа N, и числом, образуемым оставшимися его цифрами (или наоборот), делилась соответственно на 7, 11 или 13.

При $m = 3$ будет $10^3 - 1 = 999 = 3 \cdot 9 \cdot 37$, получаем общий признак делимости на 3, 9, 37: чтобы число N делилось на 3, 9 или 37, достаточно, чтобы сумма числа, образуемого первыми тремя цифрами числа N, и числа, образуемого оставшимися его цифрами, делилась соответственно на 3, 9 или 37.

246. а) 1) 973—126 = 847.

847 делится на 7, следовательно, и число N делится на 7;

847 делится на 11, следовательно, и число N делится на 11;

847 не делится на 13, следовательно, и число N не делится на 13.

3) 96 736 — 69 = 96 668. К числу 96 668 снова применяем взятый признак, но вычитаем 96 из 668: 668 — 96 = 572; 572 делится на 11, следовательно, 96 736 068 делится на 11; 572 делится на 13, следовательно, 96 736 068 делится на 13.

б) 1) 794 + 20 = 814 делится на 37, следовательно, число N делится на 37.

3) 2575 + 163 = 2738; 738 + 2 = 740 делится на 37, следовательно, число N делится на 37.

247. Пусть N — натуральное число по десятичной системе счисления и M — сумма его цифр.

В силу известного признака делимости на 9

$$N \equiv M \pmod 9.$$

Пусть

$$\left.\begin{aligned} N_1 &\equiv M_1 \\ N_2 &\equiv M_2 \end{aligned}\right\} \pmod 9;$$

тогда

$$N_1 \pm N_2 \equiv M_1 \pm M_2 \pmod 9, \qquad (1)$$

или, обозначая $M_1 \pm M_2$ через M, получаем:

$$N_1 \pm N_2 \equiv M \pmod 9. \qquad (2)$$

Из (1) и (2) следует:

$$M_1 \pm M_2 \equiv M \pmod 9,$$

т. е. если сложение или вычитание выполнено верно, то сумма или разность цифр компонент сравнима с суммой цифр результата.

Совершенно аналогично рассуждая, для действия умножения имеем:

$$M_1 \cdot M_2 \ldots M_k \equiv M \pmod 9,$$

т. е. если умножение выполнено верно, то произведение сумм цифр сомножителей сравнимо с суммой цифр результата.

Результат деления проверяется с помощью контроля умножения.

248. 1) $12 + 23 = 35 \equiv 17 \pmod 9$, $35 - 17 = 18$ делится на 9, следовательно, сложение выполнено верно.

4) $20 \cdot 8 = 160 \equiv 34 \pmod 9$, $160 - 34 = 126$ делится на 9, следовательно, умножение выполнено верно.

7) $37 \equiv 7 \cdot 49 = 343 \pmod 9$, $343 - 37 = 306$ делится на 9, следовательно, деление выполнено верно.

§ 22. Конечные непрерывные дроби

249. 1)

$$\frac{29}{37} = (0, 1, 3, 1, 1, 1, 2).$$

$$\begin{array}{rl|l}
 & 29 & 37 \\
37 & 29 & 0 = q_0 \\
29 & 8 & 1 = q_1 \\
8 & 5 & 3 = q_2 \\
5 & 3 & 1 = q_3 \\
3 & 2 & 1 = q_4 \\
2 & 1 & 1 = q_5 \\
\hline
0 & 2 = q_6 &
\end{array}$$

По схеме составляем подходящие дроби:

q_s			0	1	3	1	1	1	2
P_s	0	1	0	1	3	4	7	11	29
Q_s	1	0	1	1	4	5	9	14	37

$$\frac{P_4}{Q_4} = \frac{7}{9},$$

$$\frac{1}{Q_4 Q_5} = \frac{1}{9 \cdot 14} = \frac{1}{126} \approx 0{,}008 < 0{,}01;$$

$$\frac{7}{9} \approx 0{,}78 \text{ с избытком.}$$

Итак, $\frac{29}{37} \approx \frac{7}{9} (+ 0{,}01) = 0{,}78.$

Погрешность берем со знаком $+$ потому, что $\frac{P_4}{Q_4} < \frac{a}{b}$. Частное

от деления 7 на 9 берем с избытком потому, что $\frac{7}{9}$ является приближением с недостатком.

В десятичном приближении $\frac{29}{37} \approx 0{,}78$ погрешность не указываем, так как ее нужно вычислять особо, как сумму погрешности $+\ 0{,}008$ и погрешности округления частного при делении 7 на 9.

3) $\frac{648}{385} \approx \frac{69}{41}\ (+\ 0{,}0003) \approx 1{,}6830.$

4) $\frac{571}{359} \approx \frac{35}{22}\ (-\ 0{,}0005) \approx 1{,}5909.$

250. 1) Составляем подходящие дроби по схеме:

q_s			2	1	1	3	1	2
P_s	0	1	2	3	5	18	23	64
Q_s	1	0	1	1	2	7	9	25

$\frac{a}{b} = \frac{64}{25}$.

Можно решение выполнить и так:

$$\frac{a}{b} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{2}}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{2}{3}}}} =$$

$$= 2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{3}{11}}} = 2 + \cfrac{1}{1 + \frac{11}{14}} = 2 + \frac{14}{25} = \frac{64}{25},$$

но этот путь решения удобен только при небольшом количестве частных $q_0, q_1, \ldots, q_n$.

2) $\frac{73}{43}$. 4) $\frac{2633}{1810}$.

251. 1)

$$\begin{array}{r|l} 3587 & 2743 \\ \hline 2743 & 1 = q_0 \end{array}$$

$$\begin{array}{r|l} 2743 & 844 \\ \hline 2532 & 3 = q_1 \end{array}$$

$$\begin{array}{r|l} 844 & 211 \\ \hline 844 & 4 = q_2 \\ \hline 0 & \end{array}$$

$$\frac{3587}{2743} = 1 + \cfrac{1}{3 + \frac{1}{4}} = 1 + \frac{4}{13} = \frac{17}{13}.$$

Как видим, сокращение происходит без выполнения процесса деления числителя и знаменателя дроби на их наибольший общий делитель 211.

3) $\dfrac{3653}{3107} = \dfrac{281}{239}$.

252. Задача сводится к замене данной дроби подходящей дробью с погрешностью замены, не превышающей 0,001. Разлагаем данную дробь в непрерывную:

$$\begin{array}{r|l} 587 & 113 \\ \hline 565 & 5 = q_0 \end{array}$$

$$\begin{array}{r|l} 113 & 22 \\ \hline 110 & 5 = q_1 \end{array}$$

$$\begin{array}{r|l} 22 & 3 \\ \hline 21 & 7 = q_2 \end{array}$$

$$\begin{array}{r|l} 3 & 1 \\ \hline 3 & 3 = q_3 \\ \hline 0 & \end{array}$$

Составляем подходящие дроби по схеме:

q_s			5	5	7	3
P_s	0	1	5	26	187	587
Q_s	1	0	1	5	36	113

Если возьмем для замены дробь $\dfrac{26}{5}$, то погрешность будет $\dfrac{1}{5 \cdot 36} = \dfrac{1}{180} \approx 0{,}006$, более заданной 0,001, поэтому дробь $\dfrac{26}{5}$ не подходит.

Берем дробь $\dfrac{187}{36}$. Находим погрешность:

$$\frac{1}{36 \cdot 113} = \frac{1}{4068} \approx 0{,}0003 < 0{,}001.$$

Итак, можно построить передачу при помощи шестерен с меньшим количеством зубцов, что технически возможно (погрешность не превышает заданную), является более удобным (меньше зубцов) и более прочным (зубцы крупнее).

253. Возьмем сначала уравнение:

$$ax + by = 1, \quad \text{где} \quad (a, b) = 1.$$

Представим дробь $\dfrac{a}{b}$ в виде непрерывной дроби:

$$\frac{a}{b} = (q_0, q_1, q_2, \ldots, q_n).$$

По формуле разности между двумя подходящими дробями имеем:

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_n Q_{n-1}},$$

но

$$\frac{P_n}{Q_n} = \frac{a}{b},$$

поэтому

$$\frac{a}{b} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{b\,Q_{n-1}},$$

откуда

$$a\,Q_{n-1} - b\,P_{n-1} = (-1)^{n-1},$$

или

$$a\,(-1)^{n-1}\,Q_{n-1} + b\,(-1)^n\,P_{n-1} = 1.$$

Сопоставляя найденное равенство с уравнением $ax + by = 1$, получаем:

$$x = (-1)^{n-1}\,Q_{n-1}, \quad y = (-1)^n\,P_{n-1}.$$

Если возьмем уравнение $ax + by = c$, то получим:

$$x = (-1)^{n-1}\,Q_{n-1}\,c \quad \text{и} \quad y = (-1)^n\,P_{n-1}\,c.$$

Если в уравнении коэффициент b будет со знаком минус, то, очевидно, в формуле для y нужно брать $(-1)^{n-1}$.

Подставляя найденные значения x и y в формулы $x = x_1 - bt$ и $y = y_1 + at$ вместо x_1 и y_1, найдем общее решение уравнения

$$ax + by = c.$$

254. 1) Разлагая дробь $\frac{38}{117}$ в непрерывную, получим $\frac{38}{117} = (0, 3, 12, 1, 2)$. Находим подходящие дроби по схеме:

q_s			0	3	12	1	2
P_s	0	1	0	1	12	13	38
Q_s	1	0	1	3	37	40	117

Имеем: $P_{n-1} = 13$, $Q_{n-1} = 40$, $n = 4$. По формулам получаем:

$$x_1 = (-1)^3\,40 \cdot 209 = -8360,$$
$$y_2 = (-1)^4 \cdot 13 \cdot 209 = 2717.$$

Общее решение:

$$x = -8360 - 117\,t,$$
$$y = 2717 + 38\,t.$$

Проверка. $38\,(-8360) + 117 \cdot 2717 = -317\,680 + 317\,889 = 209.$

3) Разлагая дробь $\frac{119}{68}$ в непрерывную, получим: $\frac{119}{68} = (1, 1, 3)$.

Находить подходящие дроби удобнее по схеме:

q_s			1	1	3
P_s	0	1	1	2	7
Q_s	1	0	1	1	4

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

Видим, что $(119, 68) = 17$ и $c = 34$ делится на 17. Сокращая члены уравнения, получаем:

$$7x - 4y = 2.$$

По формулам находим:

$$x_1 = (-1)^1 1 \cdot 2 = -2; \quad y_1 = (-1)^1 \cdot 2 \cdot 2 = -4.$$

Общее решение:

$$\left.\begin{aligned} x &= -2 + 4t, \\ y &= -4 + 7t. \end{aligned}\right\}$$

Проверка. $7 \cdot (-2) - 4 \cdot (-4) = -14 + 16 = 2$.

5) $x = -125 - 114t$, $y = 45 + 41t$.

§ 23. Бесконечные непрерывные дроби; квадратичные иррациональности

255. 1) Целая часть $\sqrt{11}$ есть 3, поэтому $\sqrt{11} = 3 + \frac{1}{\omega_1}$, откуда $\omega_1 = \frac{1}{\sqrt{11}-3} = \frac{\sqrt{11}+3}{(\sqrt{11}-3)(\sqrt{11}+3)} = \frac{\sqrt{11}+3}{2}$. Целая часть числа $\frac{\sqrt{11}+3}{2}$ есть 3, поэтому $\frac{\sqrt{11}+3}{2} = 3 + \frac{1}{\omega_2}$, откуда $\omega_2 = \frac{2}{\sqrt{11}-3} = \frac{2(\sqrt{11}+3)}{(\sqrt{11}-3)(\sqrt{11}+3)} = \sqrt{11}+3$. Целая часть $\sqrt{11}+3$ равна 6, поэтому $\sqrt{11}+3 = 6 + \frac{1}{\omega_3}$, откуда $\omega_3 = \frac{1}{\sqrt{11}-3} = \frac{\sqrt{11}+3}{2} = \omega_1$. Получаем:

$$\sqrt{11} = 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{6 + \ldots}}}},$$

или в краткой записи $\omega = \sqrt{11} = [3, (3, 6)]$.

Находим подходящие дроби по схеме:

q_s			3	3	6	3	6	...
P_s	0	1	3	10	63	199	1257	...
Q_s	1	0	1	3	19	60	379	...

Определяем погрешность:

$$\frac{1}{Q_3Q_4}=\frac{1}{60\cdot 379}=\frac{1}{22470}\approx 0{,}00005.$$

Берем $\frac{P_3}{Q_3}=\frac{199}{60}\approx 3{,}3166$ с недостатком. Итак, $\sqrt{11}\approx\frac{199}{60}(-0{,}00005)\approx$ $\approx 3{,}3166$ (см. конец решения примера 1 из задачи 249).

3) $\sqrt{12}\approx\frac{97}{28}(-0{,}0002)\approx 3{,}4642.$

5) $1+\sqrt{7}\approx\frac{51}{14}(+0{,}005)\approx 3{,}643.$

7) Разлагая число $\omega=\frac{1+\sqrt{3}}{2}$ в непрерывную дробь, получаем:

$$\frac{1+\sqrt{3}}{2}=[(1,2)].$$

Находим подходящие дроби по схеме:

q_s			1	2	1	2	1	2	1	2	1	...
P_s	0	1	1	3	4	11	15	41	56	153	209	...
Q_s	1	0	1	2	3	8	11	30	41	112	153	...

$Q_7=112>100$, поэтому берем дробь $\frac{P_7}{Q_7}=\frac{153}{112}\approx 1{,}36607$ с недостатком. Находим погрешность:

$$\frac{1}{Q_7Q_8}=\frac{1}{112\cdot 153}\approx 0{,}00006.$$

Имеем:

$$\frac{1+\sqrt{3}}{2}\approx\frac{153}{112}(-0{,}00006)\approx 1{,}36607.$$

256. 1) Разлагая число $\sqrt{3}$ в непрерывную дробь, получаем $\sqrt{3}=[1,(1,2)]$. Находим подходящие дроби по схеме:

q_s			1	1	2	1	2	1	2	1	2	1	...
P_s	0	1	1	2	5	7	19	26	71	97	265	362	...
Q_s	1	0	1	1	3	4	11	15	41	56	153	209	...

Возьмем для пробы дробь $\frac{P_7}{Q_7}=\frac{97}{56}$. Погрешность будет равна $\frac{1}{56\cdot 153}\approx 0{,}00012>0{,}0001$, не удовлетворяет условию.

Берем дробь $\frac{P_8}{Q_8}=\frac{165}{153}\approx 1{,}73203$ с избытком.

Находим погрешность: $\frac{1}{153\cdot 209}=\frac{1}{31977}\approx 0{,}00003<0{,}0001$.

Эта погрешность удовлетворяет требованию точности замены. Получаем:

$$\sqrt{3}\approx\frac{165}{153}(+0{,}00003)\approx 1{,}73203.$$

3) $\sqrt{6}\approx\frac{218}{89}(+0{,}00006)\approx 2{,}44944$.

5) $\frac{2+\sqrt{5}}{3}=1+\frac{1}{\omega_1}$, $\omega_1=\frac{3}{\sqrt{5}-1}=\frac{3(\sqrt{5}+1)}{4}=\frac{\sqrt{45}+3}{4}$;

$\frac{\sqrt{45}+3}{4}=2+\frac{1}{\omega_2}$, $\omega_2=\frac{4}{\sqrt{45}-5}=\frac{\sqrt{45}+5}{5}$; продолжая разложение, получаем:

$$\frac{2+\sqrt{5}}{3}=[1,(2,2,2,1,12,1)].$$

Составляем подходящие дроби:

q_s			1	2	2	2	1	12	1	...
P_s	0	1	1	3	7	17	24	305	329	...
Q_s	1	0	1	2	5	12	17	216	233	...

Вычисляем погрешность:

$$\frac{1}{Q_5Q_6}=\frac{1}{216\cdot 233}=\frac{1}{50328}\approx 0{,}00002<0{,}0001;$$

она удовлетворяет условию.

Берем $\frac{P_5}{Q_5}=\frac{305}{216}\approx 1{,}41203$ с недостатком. Получаем: $\frac{2+\sqrt{5}}{3}\approx$

$\approx\frac{305}{216}(-0{,}00002)\approx 1{,}41203$.

7) $\dfrac{2+\sqrt{14}}{4} \approx \dfrac{89}{62}(-0{,}00008) \approx 1{,}43548.$

257. 1) В том случае, когда перед квадратным корнем стоит знак минус, целая часть корня берется такой, чтобы квадрат ее был больше подкоренного числа. В данном примере в качестве целой части числа $-\sqrt{15}$ берем -4; имеем:

$$5-\sqrt{15}=1+\frac{1}{\omega_1},\quad \omega_1=\frac{1}{4-\sqrt{15}}=4+\sqrt{15};$$

$$4+\sqrt{15}=7+\frac{1}{\omega_2},\quad \omega_2=\frac{1}{\sqrt{15}-3}=\frac{\sqrt{15}+3}{6};$$

продолжая разложение дальше, получаем:

$$5-\sqrt{15}=[1,7,(1,6)].$$

Составляем подходящие дроби:

q_s			1	7	1	6	1	6	...
P_s	0	1	1	8	9	62	71	488	...
Q_s	1	0	1	7	8	55	63	433	...

Вычисляем погрешность:

$$\frac{1}{Q_4Q_5}=\frac{1}{63\cdot 433}=\frac{1}{27279}\approx 0{,}00004<0{,}0001.$$

Берем $\dfrac{P_4}{Q_4}=\dfrac{71}{63}\approx 1{,}12698$ с избытком. Итак, $5-\sqrt{15}\approx\dfrac{71}{69}(+0{,}00004)\approx$ $\approx 1{,}12698.$

3) $\dfrac{3-\sqrt{7}}{5}=0+\dfrac{1}{\omega_1},\quad \omega_1=\dfrac{5}{3-\sqrt{7}}=\dfrac{5(3+\sqrt{7})}{2}=\dfrac{15+\sqrt{175}}{2};$

$$\frac{15+\sqrt{175}}{2}=14+\frac{1}{\omega_2},\quad \omega_2=\frac{2}{\sqrt{175}-13}=\frac{\sqrt{175}+13}{3}.$$

Продолжая процесс дальше, получаем:

$$\frac{3-\sqrt{7}}{3}=[0,14,(8,1,2,1,8,13)].$$

Составляем подходящие дроби:

q_s			0	14	8	1	2	...
P_s	0	1	0	1	8	9	26	...
Q_s	1	0	1	14	113	127	367	...

Вычисляем погрешность:

$$\frac{1}{Q_3Q_4} = \frac{1}{113\cdot 127} = \frac{1}{14351} \approx 0{,}00007 < 0{,}0001.$$

Берем $\frac{P_3}{Q_3} = \frac{8}{113} \approx 0{,}07080$ с избытком. Получаем:

$$\frac{3-\sqrt{5}}{5} \approx \frac{8}{113}(+0{,}00007) \approx 0{,}07080.$$

5) $1-\sqrt{31} = -5+\frac{1}{\omega_1}$, $\omega_1 = \frac{1}{6-\sqrt{31}} = \frac{6+\sqrt{31}}{5}$,

$$\frac{6+\sqrt{31}}{5} = 2+\frac{1}{\omega_2}, \quad \omega_2 = \frac{5}{\sqrt{31}-4} = \frac{\sqrt{31}+4}{3}.$$

Продолжив процесс разложения дальше, получим:

$$1-\sqrt{31} = [-5, 2, (3, 5, 3, 1, 1, 10, 1, 1)].$$

Вычислим знаменатели подходящих дробей по схеме:

q_s			-5	2	3	5	3	1	...
Q_s	1	0	1	2	3	37	118	155	...

Если возьмем для замены подходящую дробь $\frac{P_4}{Q_4}$, то погрешность будет:

$$\frac{1}{118\cdot 155} = \frac{1}{18290} \approx 0{,}00006 < 0{,}0001$$

— удовлетворяет требованию точности замены.

Для вычисления числителя подходящей дроби $\frac{P_4}{Q_4}$ следовало бы поступать так. Берем

$$\frac{P_4}{Q_4} = -5+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{5+\frac{1}{3}}}} = -5+\frac{51}{118} = -\frac{539}{118};$$

получаем не только числитель $P_4 = 539$, но и всю дробь, но со знаком минус благодаря отрицательному $q_0 = -5$.

Однако проще и в этом случае для вычисления подходящих дробей применять схему. Так, для данного примера имеем:

q_s			-5	2	3	5	3	1	...
P_s	0	1	-5	-9	-32	-169	-539	...	...
Q_s	1	0	1	2	3	37	118	155	...

Получаем $\frac{P_4}{Q_4} = -\frac{539}{118}$.

Имеем в виду, что знаки минус перед числителями являются знаками перед самими подходящими дробями благодаря отрицательному q_0, что получается в случае замены отрицательной квадратичной иррациональности.

Берем $\frac{P_4}{Q_4} = \frac{539}{118} \approx 4{,}56780$ с избытком. Итак,

$$1 - \sqrt{31} \approx -\frac{539}{118}(+0{,}00006) \approx -4{,}56780.$$

7) $\omega = \frac{5-\sqrt{37}}{3}$. В качестве целой части числа $-\sqrt{37}$ следовало бы взять -7, но $5-7$ не делится на 3, поэтому берем -8 и получаем:

$$\frac{5-\sqrt{37}}{3} = -1 + \frac{1}{\omega_1}, \quad \omega_1 = \frac{3}{8-\sqrt{37}} = \frac{8+\sqrt{37}}{9},$$

$$\frac{8+\sqrt{37}}{9} = 1 + \frac{1}{\omega_2}, \quad \omega_2 = \frac{9}{\sqrt{37}-1} = \frac{\sqrt{37}+1}{4};$$

продолжая процесс дальше, получаем:

$$\frac{5-\sqrt{37}}{3} = [-1, 1, 1, (1, 1, 2)].$$

Находим подходящие дроби по схеме:

q_s			-1	1	1	1	1	2	1	1	2	1	1	...
P_s	0	1	-1	0	-1	-1	-2	-5	-7	-12	-31	-43	-74	...
Q_s	1	0	1	1	2	3	5	13	18	31	80	111	191	...

Погрешность: $\frac{1}{111 \cdot 191} = \frac{1}{21201} \approx 0{,}00005 < 0{,}0001$.

Берем $\frac{P_3}{Q_3} = \frac{43}{111} \approx 0{,}38738$ с недостатком. Итак,

$$\frac{5-\sqrt{37}}{3} \approx -\frac{43}{111}(-0{,}00005) \approx -0{,}038738.$$

9) $-2-\sqrt{17} = [-7, 1, 7, (8)] \approx -\frac{398}{65}(-0{,}00003) \approx -6{,}12307.$

11) $-4-\sqrt{46} = [-3, 1, 5, (2, 1, 1, 3, 1, 12, 1, 3, 1, 1, 2, 6)] \approx$
$\approx -\frac{248}{115} \cdot (+0{,}00006) \approx -2{,}15653.$

258. 1) Из условия $\omega = (1, 2, 4, 6, \omega)$.

Составляем таблицу подходящих дробей:

q_s			1	2	4	6	ω
P_s	0	1	1	3	13	81	$81\omega+13$
Q_s	1	0	1	2	9	56	$56\omega+9$

По формуле выражения ω через полное частное

$$\omega = \frac{P_{n-1}\omega_n + P_{n-2}}{Q_{n-1}\omega_n + Q_{n-2}}$$

имеем:

$$\omega = \frac{81\omega + 13}{56\omega + 9},$$

откуда

$$56\omega^2 + 9\omega = 81\omega + 13,$$

или

$$56\omega^2 - 72\omega - 13 = 0.$$

Решая уравнение, получаем:

$$\omega = \frac{18 \pm \sqrt{506}}{28}.$$

Так как $\omega = [(1, 2, 4, 6)]$ — число положительное, то берем положительный корень и окончательно находим:

$$[(1, 2, 4, 6)] = \frac{18 + \sqrt{506}}{28}.$$

3) $(2, 2, 1, 1) = \frac{9 + \sqrt{221}}{10}$.

4) Из условия имеем:

$$\omega = (2, \omega_1), \tag{1}$$

$$\omega_1 = (1, 1, 1, 4, \omega_1). \tag{2}$$

Из (1) получаем:

$$\omega = 2 + \frac{1}{\omega_1},$$

откуда

$$\omega_1 = \frac{1}{\omega - 2}. \tag{1'}$$

Для (2) удобнее составить схему:

q_s			1	1	1	4	ω_1
P_s	0	1	1	2	3	14	$14\omega_1 + 3$
Q_s	1	0	1	1	2	9	$9\omega_1 + 2$

Получаем $\omega_1 = \dfrac{14\omega_1 + 3}{9\omega_1 + 2}$. Подставляя значение ω_1 из (1′) в (2′), имеем:

$$\frac{1}{\omega - 2} = \frac{\dfrac{14}{\omega - 2} + 3}{\dfrac{9}{\omega - 2} + 2},$$

или после преобразований:

$$\frac{1}{\omega - 2} = \frac{3\omega + 8}{2\omega + 5},$$

откуда $3\omega^2 = 21$, $\omega^2 = 7$, $\omega = \pm\sqrt{7}$.

Берем положительное значение корня и получаем:

$$[2, (1, 1, 1, 4)] = \sqrt{7}.$$

Другое решение. Из условия по-прежнему имеем: $\omega = (2, \omega_1)$, или

$$\omega = 2 + \frac{1}{\omega_1}, \tag{1}$$

$$\omega_1 = (1, 1, 1, 4, \omega_1). \tag{2}$$

Из (2) по схеме находим:

$$\omega_1 = \frac{14\omega_1 + 3}{9\omega_1 + 2},$$

откуда после преобразований получаем уравнение:

$$3\omega_1^2 - 4\omega_1 - 1 = 0,$$

решая которое, имеем:

$$\omega_1 = \frac{2 + \sqrt{7}}{3}.$$

Берем в качестве ω_1 положительный корень

$$\omega_1 = \frac{2 + \sqrt{7}}{3}$$

и подставляем в (1):

$$\omega = 2 + \frac{1}{\dfrac{2 + \sqrt{7}}{3}} = 2 + \frac{3}{2 + \sqrt{7}} = \frac{7 + 2\sqrt{7}}{2 + \sqrt{7}} =$$

$$= \frac{(7 + 2\sqrt{7})(2 - \sqrt{7})}{-3} = \frac{(7 + 2\sqrt{7})(\sqrt{7} - 2)}{3} = \frac{3\sqrt{7}}{3} = \sqrt{7}.$$

Способ является менее удобным из-за операции освобождения от иррациональности в знаменателе, особенно при больших числах.

259. 1) Из условия имеем:

$$\omega = (1, 1, 2, 2, 1, \omega).$$

Составляем таблицу подходящих дробей:

q_s			1	1	2	2	1	ω
P_s	0	1	1	2	5	12	17	$17\omega + 12$
Q_s	1	0	1	1	3	7	10	$10\omega + 7$

Отсюда

$$\omega = \frac{17\omega + 12}{10\omega + 7},$$

или

$$10\omega^2 - 17\omega - 5 = 0.$$

Бóльшим корнем этого уравнения и является данная непрерывная чистая периодическая дробь:

$$[(1, 1, 2, 2, 1)] = \frac{17 + \sqrt{489}}{20}.$$

4) Бóльшим корнем уравнения $\omega^2 - \omega - 4 = 0$.

260. 1) Решая уравнение, находим:

$$x_{1,2} = \frac{15 \pm \sqrt{17}}{4}.$$

Вычисляем первый корень x_1. Представляя x_1 непрерывной дробью, получаем:

$$x_1 = [4, (1, 3, 1,)].$$

Составляем подходящие дроби по схеме:

q_s			4	1	3	1	1	3	1	1	3	...
P_s	0	1	4	5	19	24	43	153	196	349	1243	...
Q_s	1	0	1	1	4	5	9	32	41	79	260	...

Так как $\frac{1}{Q_7 Q_8} = \frac{1}{79 \cdot 260} \approx 0{,}00006 < 0{,}0001$, то берем $\frac{P_7}{Q_7} = \frac{349}{73} \approx 4{,}7808$ с недостатком и получаем $x_1 \approx \frac{349}{73} (- 0{,}0001) \approx 4{,}7808$.

Вычислим второй корень. Представляя x_2 непрерывной дробью, получаем:

$$x_2 = [2, 1, 2, (1, 1, 3)].$$

Составляем подходящие дроби:

q_s			2	1	2	1	1	3	1	1	3	...
P_s	0	1	2	3	8	11	19	68	87	155	552	...
Q_s	1	0	1	1	3	4	7	25	32	57	203	...

Так как $\frac{1}{Q_7 Q_8} = \frac{1}{57 \cdot 203} \approx 0{,}00009 < 0{,}0001$, то берем $\frac{P_7}{Q_7} = \frac{155}{57} \approx 2{,}7192$ с недостатком; получаем:

$$x_2 \approx \frac{155}{57}(-0{,}0001) \approx 2{,}7192.$$

3) Решая уравнение, находим:

$$x_{1,2} = \frac{-9 \pm \sqrt{57}}{2}.$$

Вычисляем первый корень. Разлагая x_1 в непрерывную дробь, получаем:

$$x_1 = [-1, 3, (1, 1, 1, 3, 7, 3)].$$

Составляем подходящие дроби:

q_s			−1	3	1	1	1	3	7	...
P_s	0	1	−1	−2	−3	−5	−8	−29	−211	...
Q_s	1	0	1	3	4	7	11	40	291	...

Так как $\frac{1}{Q_5 Q_6} = \frac{1}{40 \cdot 291} \approx 0{,}00009 < 0{,}0001$, то берем $\frac{P_5}{Q_5} = \frac{29}{40} \approx 0{,}7250$ с недостатком, получаем:

$$x_1 \approx -\frac{29}{40}(-0{,}0001) \approx -0{,}7250.$$

Вычисляем второй корень. Разлагая x_2 в непрерывную дробь, получаем:

$$x_2 = [-9, 1, 2, (1, 1, 1, 3, 7, 3)].$$

Составляем подходящие дроби:

q_s			−9	1	2	1	1	1	3	7	...
P_s	0	1	−9	−8	−25	−33	−58	−91	−331	−2408	...
Q_s	1	0	1	1	3	4	7	11	40	291	...

Так как $\frac{1}{Q_7Q_8} = \frac{1}{40 \cdot 291} \approx 0{,}00009 < 0{,}0001$, то берем $\frac{P_7}{Q_7} = -\frac{331}{40} \approx 8{,}2750$ с недостатком, получаем:

$$x_2 \approx -\frac{331}{40}(-0{,}0001) \approx -8{,}2750^*.$$

5) $x_1 \approx -\frac{211}{80}(-0{,}0001) \approx -2{,}6375$,

$$x_2 \approx \frac{311}{301}(-0{,}0001) \approx -1{,}0332.$$

261. Положим

$$\cfrac{1}{b+\cfrac{1}{a+\cfrac{1}{b+\cfrac{1}{a+}}}} \\ \cdots = x, \qquad (1)$$

тогда требуется доказать, что

$$x(a+x) = \frac{a}{b}.$$

Из (1) находим $x = \cfrac{1}{b+\cfrac{1}{a+x}}$,

откуда после преобразований получаем:

$$x^2 + ax - \frac{a}{b} = 0, \quad \text{или} \quad (a+x)x = \frac{a}{b},$$

что и требовалось доказать.

262. Имеем: $\sqrt{a^2+a+1} = a + \sqrt{a^2+a+1} - a = a + \\ + \frac{a^2+a+1-a^2}{\sqrt{a^2+a+1}+a} = a + \cfrac{1}{\cfrac{\sqrt{a^2+a+1}+a}{a+1}}$,

$$\frac{\sqrt{a^2+a+1}+a}{a+1} = \frac{(a+1)+\sqrt{a^2+a+1}-1}{a+1} = \\ = 1 + \frac{a^2+a+1-1}{(a+1)(\sqrt{a^2+a+1}+1)} = 1 + \cfrac{1}{\cfrac{\sqrt{a^2+a+1}+1}{a}};$$

* Ограничиваясь вычислением корней только квадратных уравнений, мы не рассматриваем и не применяем способ Лагранжа.

$$\frac{\sqrt{a^2+a+1}+1}{a} = \frac{a+\sqrt{a^2+a+1}+1-a}{a} =$$

$$= 1 + \frac{\sqrt{a^2+a+1}-(a-1)}{a} = 1 + \frac{1}{\dfrac{\sqrt{a^2+a+1}+a-1}{3}}.$$

Итак,

$$\sqrt{a^2+a+1} = a + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{\dfrac{\sqrt{a^2+a+1}+a-1}{3}}}}$$

Находим подходящие дроби по схеме:

q_s			a	1	1	...
P_s	0	1	a	$a+1$	$2a+1$	...
Q_s	1	0	1	1	2	...

Отсюда $\dfrac{P_2}{Q_2} = \dfrac{2a+1}{2}$.

263. Имеем: $\sqrt{x^2+1} = x + \sqrt{x^2+1} - x = x + \dfrac{1}{\sqrt{x^2+1}+x}$,

$$\sqrt{x^2+1}+x = 2x + \sqrt{x^2+1} - x = 2x + \frac{1}{\sqrt{x^2+1}+x}.$$

Следовательно, $\sqrt{x^2+1} = [x, (2x)]$.

Составляем подходящие дроби:

q_s			x	$2x$	$2x$	...
P_s	0	1	x	$2x^2+1$	$4x^3+3x$	...
Q_s	1	0	1	$2x$	$4x^2+1$	...

Получаем $\dfrac{P_2}{Q_2} = \dfrac{4x^3+3x}{4x^2+1}$.

§ 24. Алгебраические и трансцендентные числа

264. 1) Число $\dfrac{3}{5}$ является корнем уравнения

$$x - \frac{3}{5} = 0, \quad \text{или} \quad 5x - 3 = 0$$

с рациональными коэффициентами, левая часть которого не приводима в поле рациональных чисел. Следовательно, число $\frac{3}{5}$ является алгебраическим числом первой степени.

3) Число $\sqrt{3}$ является алгебраическим второй степени как корень уравнения $x^2 - 3 = 0$.

5) Слагаемые данного числа $1 + \sqrt{2}$ являются алгебраическими числами, следовательно, число $1 + \sqrt{2}$ является алгебраическим уже потому, что представляет собой сумму алгебраических чисел.

Чтобы установить степень числа $1 + \sqrt{2}$, поступаем так.

Составляем квадратный трехчлен, корнями которого являются числа $1 \pm \sqrt{2}$: $[x - (1 + \sqrt{2})][x - (1 - \sqrt{2})] = x^2 - 2x - 1$; число $1 + \sqrt{2}$ является корнем уравнения $x^2 - 2x - 1 = 0$ с рациональными коэффициентами, левая часть которого не приводима в поле рациональных чисел. Следовательно, число $1 + \sqrt{2}$ является алгебраическим числом второй степени.

7) Число $2 + i$ является алгебраическим второй степени как корень уравнения $x^2 - 4x + 5 = 0$.

9) Число $\sqrt{3} + \sqrt{5}$ является алгебраическим как сумма алгебраических чисел. Установим степень его. Возьмем число $\sqrt{3} - \sqrt{5}$. Составим квадратный трехчлен, корнями которого являются числа $\sqrt{3} \pm \sqrt{5}$:

$$[x - (\sqrt{3} + \sqrt{5})][x - (\sqrt{3} - \sqrt{5})] = x^2 - 2\sqrt{3}x - 2.$$

Полученный трехчлен имеет не все коэффициенты рациональными. Составим многочлен с рациональными коэффициентами следующим образом:

$$[(x^2 - 2) - 2\sqrt{3}x][(x^2 - 2) + 2\sqrt{3}x] = x^4 - 16x^2 + 4.$$

Теперь ясно, что число $\sqrt{3} + \sqrt{5}$ является корнем полученного многочлена или, что то же, уравнения

$$x^4 - 16x^2 + 4 = 0$$

с рациональными коэффициентами, левая часть которого не приводима в поле рациональных чисел. Следовательно, число $\sqrt{3} + \sqrt{5}$ является алгебраическим четвертой степени.

265. 1) Все коэффициенты уравнения являются рациональными числами, и левая часть его представляет собой многочлен, не приводимый в поле рациональных чисел (по теореме Эйзенштейна*). Следовательно, все корни данного уравнения являются алгебраическими числами третьей степени.

266. 1) Так как 3 — алгебраическое число, отличное от 0 и 1, и $\sqrt{2}$ — алгебраическое число второй степени, то по теореме Гельфонда число $3^{\sqrt{2}}$ трансцендентно.

---

* См.: Окунев Л., Я.. *Высшая алгебра*, 1958, стр. 237 или Курош А. Г., *Курс высшей алгебры*, 1963, стр. 353.

ТАБЛИЦЫ

Таблица простых чисел в пределах первой тысячи

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

Таблица квадратов натуральных чисел от 1 до 99

	0	1	2	3	4	5	6	7	8	9
0	0	1	4	9	16	25	36	49	64	81
1	100	121	144	169	196	225	256	289	324	361
2	400	441	484	529	576	625	676	729	784	841
3	900	961	1024	1089	1156	1225	1296	1369	1444	1521
4	1600	1681	1764	1849	1936	2025	2116	2209	2304	2401
5	2500	2601	2704	2809	2916	3025	3136	3249	3364	3481
6	3600	3721	3844	3969	4096	4225	4356	4489	4624	4761
7	4900	5041	5184	5329	5476	5625	5776	5929	6084	6241
8	6400	6561	6724	6889	7056	7225	7396	7569	7744	7921
9	8100	8281	8464	8649	8836	9025	9216	9409	9604	9801

Таблицы индексов и антииндексов

Простое число 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

i	0	1	2	3	4	5	6	7	8	9
0	1	2								

Простое число 5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Простое число 7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

i	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Простое число 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

Простое число 13

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Простое число 17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

i	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Простое число 19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Простое число 23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

i	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Простое число 29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

i	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Простое число 31

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

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

Простое число 37

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

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

Простое число 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

i	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Простое число 43

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

i	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Простое число 47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

i	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Простое число 53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

t	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

Простое число 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

t	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

Простое число 61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

t	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

Простое число 67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

t	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Простое число 71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

i	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

Простое число 73

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

i	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Простое число 79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

i	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Простое число 83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

t	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Простое число 89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

t	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Простое число 97

N	0	1	2	3	4	3	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

t	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

СОДЕРЖАНИЕ

Василий Устинович Грибанов,
Петр Иванович Титов

СБОРНИК УПРАЖНЕНИЙ ПО ТЕОРИИ ЧИСЕЛ

Редактор *В. В. Гольдберг*
Переплет художника *М. Л. Компанейца*
Художественный редактор *А. В. Сафонов*
Технический редактор *В. И. Корнеева*
Корректор *В. Г. Соловьева*

Сдано в набор 26/II-1964 г. Подписано к печати 17/VII 1964 г. 84×108$^{1}/_{32}$. Печ. л. 9(7,56). Уч.-изд. л. 6,6. Тираж 30000 экз. Тем. план 1964 г. № 27. Заказ № 43.

Издательство «Просвещение» Государственного комитета Совета Министров РСФСР по печати. Москва, 3-й проезд Марьиной рощи, 41.

Саратовский полиграфический комбинат Росглавполиграфпрома Государственного комитета Совета Министров РСФСР по печати, г. Саратов, ул. Чернышевского, 59.

Цена без переплета 20 коп. Переплет 10 коп.