ГЛАВА I

ПРОСТЕЙШИЕ СВЕДЕНИЯ ИЗ ТЕОРИИ ЧИСЕЛ

§ 1. Целая часть, дробная часть, расстояние до ближайшего целого

1. Построить графики функций $[x]$ (целая часть x), $\{x\}$ (дробная часть x), (x) (расстояние от x до ближайшего целого) и функции $f(x)=\{x-a\}-\{x\}+a$, где $0<a<1$.

2. Доказать, что $(x)=\frac{1}{2}-\left|\{x\}-\frac{1}{2}\right|$.

3. Исследовать функцию $f(x, y)=[x+y]-[x]-[y]$.

4. Вычислить $[\sqrt{1}]+[\sqrt{2}]+\ldots+[\sqrt{n^2-1}]$.

***5.** Доказать, что целая часть числа $(\sqrt{3}+2)^n$ нечетна, при любом натуральном n.

6. Пусть $1<a<b$. Чему равен наибольший натуральный показатель k, при котором $a^k\leqslant b$.

7. Доказать, что если f — неотрицательная функция, определенная на отрезке $[a, b]$, то $\sum\limits_{a\leqslant n\leqslant b}[f(n)]$ есть число точек с целыми абсциссами n, $a\leqslant n\leqslant b$, и натуральными ординатами, расположенных под графиком функции $f(x)$ (включая сам график).

***8.** Пусть φ и ψ — две возрастающие неотрицательные взаимно обратные функции, определенные на отрезках $[a, b]$ и $[\alpha, \beta]$, где $\alpha=\varphi(a)$, $\beta=\varphi(b)$. Доказать, что

$$\sum_{a<m\leqslant b}[\varphi(m)]+\sum_{\alpha<n\leqslant\beta}[\psi(n)]=[b]\cdot[\beta]-[a]\cdot[\alpha]+N,$$

где N — число точек с целыми координатами на графике функции φ на промежутке $a<x\leqslant b$.

***9.** Пусть φ и ψ — две убывающие неотрицательные взаимно обратные функции, определенные на отрезках

$[a, b]$ и $[\beta, \alpha]$, где $\alpha = \varphi(a)$, $\beta = \varphi(b)$. Доказать, что

$$\sum_{a < m \leqslant b} [\varphi(m)] - \sum_{\beta < n \leqslant \alpha} [\psi(n)] = [b]\cdot[\beta] - [a]\cdot[\alpha].$$

10. Вычислить $\sum_{k=1}^{m} [\sqrt{k}]$.

***11.** Доказать теорему: для того чтобы последовательности чисел $[\alpha x]$ и $[\beta y]$, $\alpha > 0$, $\beta > 0$, $x = 1, 2, 3, \ldots$, $y = 1, 2, 3, \ldots$, заполняли натуральный ряд без пропусков и повторений, необходимо и достаточно, чтобы α и β были иррациональны и связаны соотношением $\frac{1}{\alpha} + \frac{1}{\beta} = 1$.

§ 2. Наибольший общий делитель

12. Найти наибольший общий делитель пар чисел: a) 321 и 843; b) 23521 и 75217; c) 6787 и 7194.

***13.** Даны натуральные числа a_0 и a_1. Строится последовательность чисел: $a_2 = |a_0 - a_1|$, $a_3 = |a_1 - a_2|$, $a_4 = |a_2 - a_3|, \ldots$ Доказать, что, начиная с некоторого места, она имеет вид $d, d, 0, d, d, 0 \ldots$, где $d = (a_0, a_1)$ — наибольший общий делитель чисел a_0 и a_1.

14. Найти наибольший общий делитель чисел, запись которых в десятичной системе состоит из m единиц и из n единиц.

***15.** Доказать, что если m и n взаимно просты, то $2^m - 1$ и $2^n - 1$ тоже взаимно просты.

16. Найти наибольший общий делитель чисел $a^n - 1$ и $a^m - 1$. Здесь a — целое, m и n — натуральные числа.

***17.** Найти наибольший общий делитель чисел $a^2 + 1$ и $2a + 3$ (a — целое число).

18. Найти линейное представление наибольшего общего делителя в примерах задачи 12.

***19.** Доказать, что наибольший общий делитель $d = (a_1, a_2, \ldots, a_k)$ нескольких целых чисел равен наибольшему общему делителю чисел a_1 и $(a_2, \ldots, a_k)$ и делится на любой общий делитель чисел $a_1, a_2, \ldots, a_k$.

***20.** Доказать, что наибольший общий делитель d нескольких целых чисел $a_1, a_2, \ldots, a_k$ допускает линейное представление:

$$d = a_1 u_1 + a_2 u_2 + \ldots + a_k u_k$$

при целых $u_1, u_2, \ldots, u_k$.

21. Доказать, что если $q_0, q_1, \ldots, q_k$ — неполные частные в алгорифме Евклида для чисел a и b:

$$\begin{aligned} a &= bq_0 + r_1, \\ b &= r_1 q_1 + r_2, \\ &\dots\dots\dots \\ r_{k-2} &= r_{k-1} q_{k-1} + r_k, \\ r_{k-1} &= r_k q_k, \end{aligned}$$

то

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{}{\ddots + \cfrac{1}{q_k}}}$$

(т. е. они определяют разложение a/b в так называемую непрерывную дробь).

22. Числа Фибоначчи определяются формулами:

$$u_0 = 1, \quad u_1 = 1, \quad u_k = u_{k-1} + u_{k-2} \quad (k \geqslant 2).$$

Доказать, что

$$\frac{a^{u_{k+2}} - 1}{a^{u_{k+1}} - 1} = a^{u_k} + \cfrac{1}{a^{u_{k-1}} + \cfrac{}{\ddots + \cfrac{1}{a^{u_1} + \cfrac{1}{a^{u_0}}}}}.$$

§ 3. Каноническое разложение на простые множители

23. Написать каноническое разложение для чисел: a) 1440; b) 1575; c) 111111.

24. Написать каноническое разложение наименьшего общего кратного чисел $1, 2, \ldots, n$.

25. Написать каноническое разложение числа $n!$.

26. Доказать, что знаменатель несократимой записи числа $2^{n-1}/n!$ есть число нечетное. Может ли числитель равняться 1?

27. Не пользуясь соображениями комбинаторики, доказать, что число $\frac{n!}{m!\,(n-m)!}$ целое.

*28. Доказать, что число $\frac{(2n-2)!}{n!\,(n-1)!}$ целое.

29. Пусть S — некоторое множество вещественных чисел. Определим следующие два действия M и m над числами из S:

$$a \mathrm{M} b = \mathrm{Max}(a, b) \text{ — большее из чисел } a \text{ и } b;$$

$$a \mathrm{m} b = \min(a, b) \text{ — меньшее из чисел } a \text{ и } b.$$

Доказать, что эти действия коммутативны, ассоциативны и связаны двумя распределительными законами:

$$(a\mathrm{m}b)\,\mathrm{M}\,c = (a\mathrm{M}c)\,\mathrm{m}\,(b\mathrm{M}c),$$

$$(a\mathrm{M}b)\,\mathrm{m}\,c = (a\mathrm{m}c)\,\mathrm{M}\,(b\mathrm{m}c).$$

Доказать, что $(a\mathrm{m}b) + (a\mathrm{M}b) = a + b$.

30. Пусть $a = \prod p^{\alpha_p}$ и $b = \prod p^{\beta_p}$ — канонические разложения натуральных чисел a и b. Доказать, что наибольший общий делитель этих чисел (a, b) равен $\prod p^{\alpha_p \mathrm{m} \beta_p}$, а наименьшее общее кратное $[a, b]$ равно $\prod p^{\alpha_p \mathrm{M} \beta_p}$.

31. Доказать (для натуральных a_1, a_2, a_3):

$$(a_1, a_2)\,[a_1, a_2] = a_1 a_2;$$

$$(a_1, [a_2, a_3]) = [(a_1, a_2), (a_1, a_3)];$$

$$[a_1, (a_2, a_3)] = ([a_1, a_2], [a_1, a_3]).$$

32. Записать наименьшее общее кратное трех натуральных чисел, пользуясь действиями умножения и взятия наибольшего общего делителя.

***33.** Пусть M — некоторое конечное множество натуральных чисел, M_i — все его непустые подмножества, $d(M_i)$ — наибольший общий делитель чисел множества M_i, $\varepsilon_i = 1$ или -1, в зависимости от четности или нечетности числа элементов в M_i. Доказать, что наименьшее общее кратное чисел, составляющих множество M, равно $\prod (d(M_i))^{-\varepsilon_i}$.

34. Пусть $n \geqslant 5$ — натуральное число. Доказать, что n будет простым тогда и только тогда, когда $(n-1)!$ не делится на n.

***35.** Доказать, что существует бесконечно много простых чисел вида $4n - 1$.

36. Доказать, что если произведение двух целых взаимно простых чисел равно квадрату целого числа, то оба сомножителя — квадраты, с точностью до знака.

*37. Доказать, что если a, b — взаимно простые целые числа и $a^2+b^2=c^2$ при целом $c>0$, то найдутся такие целые числа m и n, что $a=m^2-n^2$, $b=2mn$, $c=m^2+n^2$ (или $a=2mn$, $b=m^2-n^2$).

*38. Записать в общем виде решение в целых числах уравнения $x^2+y^2=2z^2$, считая x и y взаимно простыми.

§ 4. Теория сравнений

39. Решить сравнения:

a) $2x+1\equiv 0 \pmod{13}$; b) $5x\equiv 7 \pmod{21}$; c) $10x\equiv 3 \pmod{49}$.

40. Решить сравнения:

a) $x^2\equiv -1 \pmod{13}$; b) $x^2\equiv -1 \pmod{11}$; c) $x^2\equiv 2 \pmod{31}$.

41. Решить сравнения:

a) $x^2+2x+14\equiv 0 \pmod{17}$; b) $x^2+3x+10\equiv 0 \pmod{19}$; c) $x^3-3x+1\equiv 0 \pmod{19}$; d) $x^3\equiv 5 \pmod{11}$; e) $x^3\equiv 10 \pmod{37}$.

42. Решить сравнения:

a) $6x\equiv 8 \pmod{26}$; b) $15x\equiv 12 \pmod{33}$.

***43.** Доказать, что наибольший общий делитель чисел a^2+m и $ka+l$ (a, m, k, l — целые) есть делитель числа l^2+mk^2.

***44.** Пусть $a_1, \ldots, a_{\varphi(m)}$ — наименьшие положительные вычеты из примитивных классов. Доказать, что $a_1+\ldots+a_{\varphi(m)}=\frac{1}{2}m\varphi(m)$.

45. Решить сравнение $x^2-1\equiv 0 \pmod{p^m}$ (здесь p — простое число, $p>2$, m — натуральное число).

46. Решить сравнение $x^2-1\equiv 0 \pmod{2^m}$.

47. Доказать, что если натуральные числа m_1 и m_2 взаимно просты, a_1 и a_2 — произвольные целые числа, то найдется один и только один класс чисел x по модулю m_1m_2 такой, что $x\equiv a_1 \pmod{m_1}$, $x\equiv a_2 \pmod{m_2}$.

48. Доказать, что если $m_1, m_2, \ldots, m_k$ — попарно взаимно простые, а $a_1, a_2, \ldots, a_k$ — произвольные целые числа, то найдется число $x\equiv a_i \pmod{m_i}$, однозначно определенное по модулю $m_1m_2\ldots m_k$.

49. Доказать, что сравнение $x^2-1\equiv 0 \pmod{n}$ при $n=2^{m_0}p_1^{m_1}\ldots p_k^{m_k}$ ($p_1, \ldots, p_k$ — нечетные простые числа, $m_1\geqslant 1, \ldots, m_k\geqslant 1$, $m_0\geqslant 0$) имеет 2^k решений при $m_0=0$ или $m_0=1$, 2^{k+1} решений при $m_0=2$ и 2^{k+2} решений при $m_0\geqslant 3$.

50. Доказать, что произведение всех решений сравнения $x^2-1\equiv 0 \pmod{n}$ сравнимо с 1 по модулю n, если число решений не равно 2, и сравнимо с -1, если число решений равно 2.

51. Доказать, что сравнение $x^2+1\equiv 0 \pmod{p}$ не имеет решений, если $p\equiv 3 \pmod{4}$.

***52.** Доказать, что существует бесконечно много простых чисел в прогрессии $4k+1$.

***53.** Доказать, что $(p-1)!+1\equiv 0 \pmod{p}$, если p — простое число.

***54.** Доказать сравнение $(k!)^2+(-1)^k\equiv 0 \pmod{p}$, где p — простое число, $p=2k+1$.

***55.** Пусть $\alpha_1, \ldots, \alpha_k$, где $k=\varphi(n)$, — приведенная система вычетов по модулю n. Доказать, что $\alpha_1\ldots\alpha_k\equiv -1 \pmod{n}$, если $n=4$, $n=p^m$ или $n=2p^m$ (p — нечетное простое число, $m\geqslant 1$) и $\alpha_1\ldots\alpha_k\equiv 1 \pmod{n}$ при других значениях n.

56. Найти наименьший положительный вычет числа 3^{1000} по модулю 13.

57. Пусть m — натуральное число, не делящееся на 2 и на 5. Доказать, что десятичные разложения чисел a/m при $(a, m)=1$ имеют одинаковое число цифр в периоде и это число есть делитель $\varphi(m)$.

58. Какие вычеты по модулю 19 имеют числа 7^n+11^n, $n=1, 2, 3\ldots$

59. Решить сравнение $2^n\equiv n \pmod{7}$.

***60.** Решить сравнение $2^n\equiv n \pmod{p}$, p — простое.

61. Решить сравнение $2^n\equiv n^2 \pmod{p}$, p — простое.

62. Найти вычет по модулю 7 числа

$$u_n=2^{2^{\cdot^{\cdot^{\cdot^{2}}}}},$$

в запись которого число 2 входит n раз.

***63.** Доказать, что вычеты чисел u_n по простому модулю p стабилизируются при достаточно большом n.

***64.** Пусть a и b — натуральные взаимно простые числа. Доказать, что числа $ax+by$ при целых неотрицательных x и y принимают все целые неотрицательные значения, кроме некоторых меньших ab, в количестве $\frac{(a-1)(b-1)}{2}$.

§ 5. Числовые функции

65. Функция μ со значениями $\mu(1)=1$, $\mu(p_1p_2\ldots p_k)=(-1)^k$ и $\mu(p_1^{\alpha_1}\ldots p_k^{\alpha_k})=0$, если хотя бы один показатель α_i больше единицы, называется функцией Мёбиуса. Доказать, что $\sum\limits_{d\mid n}\mu(d)=0$ при $n>1$.

***66.** Доказать тождество $\sum\limits_{1\leqslant n\leqslant x}\mu(n)\left[\frac{x}{n}\right]=1$.

***67.** Доказать следующую формулу обращения: если $f(n)=\sum\limits_{d\mid n}g(d)$, то $g(n)=\sum\limits_{d\mid n}f(d)\mu\left(\frac{n}{d}\right)$.

68. Пусть функция f мультипликативна, т. е. $f(n_1n_2)=f(n_1)f(n_2)$ при взаимно простых n_1 и n_2. Доказать, что функции $g(n)=\sum\limits_{d\mid n}f(d)$ и $h(n)=\sum\limits_{d\mid n}f(d)\mu\left(\frac{n}{d}\right)$ мультипликативны.

69. Для мультипликативной функции f доказать:

a) $f(n)=f(p_1^{\alpha_1})\ldots f(p_k^{\alpha_k})$;

b) $\sum\limits_{d\mid n}f(d)=\prod\limits_{p_i\mid d}(1+f(p_i)+\ldots+f(p_i^{\alpha_i}))$;

c) $\sum\limits_{d\mid n}f(d)\mu(d)=(1-f(p_1))\ldots(1-f(p_k))$;

d) $\sum\limits_{d\mid n}f(d)\mu\left(\frac{n}{d}\right)=(f(p_1^{\alpha_1})-f(p_1^{\alpha_1-1}))\ldots$

$\ldots(f(p_k^{\alpha_k})-f(p_k^{\alpha_k-1}))$.

Здесь $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ — каноническое разложение.

70. Исходя из формулы $\sum\limits_{d\mid n}\varphi(d)=n$ (здесь φ — функция Эйлера), вывести формулу: $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right)$. Здесь $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$.

71. Пусть $\tau(n)$ — число натуральных делителей числа n. Доказать:

a) $\tau(n)=(\alpha_1+1)\ldots(\alpha_k+1)$; b) $\sum\limits_{d\mid n}\tau(d)\mu\left(\frac{n}{d}\right)=1$;

c) $\sum\limits_{d\mid n}\tau(d)\mu(d)=(-1)^k$;

d) $\sum\limits_{d\mid n}\tau(d)=\frac{1}{2}\tau(n)\prod\limits_{i=1}^{k}(\alpha_i+2)$.

Здесь $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$.

72. Пусть $\zeta(n)$ равно сумме натуральных делителей числа n. Доказать:

a) $\zeta(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\ldots\frac{p_k^{\alpha_k+1}-1}{p_k-1}$;

b) $\sum\limits_{d\mid n}\zeta(d)\,\mu\left(\frac{n}{d}\right)=n$;

c) $\sum\limits_{d\mid n}\zeta(d)\,\mu(d)=(-1)^k p_1p_2\ldots p_k$.

*73. Доказать, что

$$\sum_{1\leqslant k\leqslant n}\tau(k)=\sum_{x=1}^{n}\left[\frac{n}{x}\right] \text{ и } \sum_{1\leqslant k\leqslant n}\tau(k)=2\sum_{x=1}^{[\sqrt{n}]}\left[\frac{n}{x}\right]-[\sqrt{n}]^2.$$

*74. Доказать, что

$$\sum_{1\leqslant k\leqslant n}\zeta(k)=\sum_{x=1}^{n}x\left[\frac{n}{x}\right]=\frac{1}{2}\sum_{y=1}^{n}\left[\frac{n}{y}\right]\cdot\left(\left[\frac{n}{y}\right]+1\right).$$

75. Пусть $f(x)$ — функция, определенная при $0<x<\infty$ и равная нулю при $x<\delta$. Положим $g(x)=\sum\limits_{k=1}^{\infty}f\left(\frac{x}{k^\alpha}\right)$, где α — вещественное число, $\alpha>0$. Доказать, что $f(x)=\sum\limits_{k=1}^{\infty}g\left(\frac{x}{k^\alpha}\right)\mu(k)$ (обе суммы в действительности конечны).

*76. Доказать, что число натуральных чисел, меньших M и свободных от квадратов (т. е. не делящихся на квадрат простого), равно $\sum\limits_{k^2\leqslant M}\mu(k)\left[\frac{M}{k^2}\right]$.

*77. Доказать, что число точек с целыми взаимно простыми координатами в квадрате $0<x\leqslant M$, $0<y\leqslant M$ равно $\sum\limits_{k\leqslant M}\mu(k)\left[\frac{M}{k}\right]^2$.

*78. Пусть $k(n)$ — число простых делителей числа n. Доказать, что $\sum\limits_{x\leqslant M}2^{k(x)}=\sum\limits_{y\leqslant M}T\left(\frac{M}{y}\right)\mu(y)$. Здесь $T(t)=\sum\limits_{z\leqslant t}\tau(z)$ (см. задачу 73).

Следующие задачи требуют знания элементов теории бесконечных рядов. Введем в рассмотрение дзета-функцию Римана $\zeta(s)=\sum\limits_{n=1}^{\infty}\frac{1}{n^s}$. Ряд, которым задается $\zeta(s)$, сходится при всех вещественных $s>1$ (он сходится и при комплексных s при $\operatorname{Re} s>1$).

79. Доказать, что $(\zeta(s))^2=\sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}$.

80. Доказать, что $\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$.

81. Доказать, что $\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1}$. Здесь p пробегает все простые числа (тождество Эйлера).

82. Выразить $\sum_{k=1}^{\infty}\frac{1}{(2k-1)^s}$ через $\zeta(s)$.

83. Выразить $\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s}$ через $\zeta(s)$.

Заметим, что этот ряд сходится, хотя и неабсолютно, и при $0<s\leqslant 1$ и его сумма является непрерывной функцией от s, $0<s<\infty$.

84. Используя задачу 83 и учитывая, что $1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots=\ln 2$, найти $\lim_{s\to 1}(s-1)\zeta(s)$.

85. Найти $\lim_{M\to\infty}\frac{1}{M}\sum_{x\leqslant M^{1/2}}\mu(x)\left[\frac{M}{x^2}\right]$ (этот предел можно истолковать, как среднюю плотность чисел, свободных от квадратов, в натуральном ряду).

***86.** Найти среднюю плотность чисел, свободных от квадратов, в прогрессиях $4k+1$ и $4k+3$.

87. Найти среднюю плотность точек на плоскости с взаимно простыми координатами среди всех точек с натуральными координатами.

§ 6. Простейшие сведения о кольцах и полях

88. Доказать, что в любом кольце с конечным числом m элементов справедливо тождество: $ma=\underbrace{a+a+\ldots+a}_{m}=0$.

89. Доказать, что кольцо (никаких предположений о свойствах умножения, кроме распределительных законов, не делается), содержащее простое число p элементов, либо изоморфно полю вычетов по модулю p, либо изоморфно аддитивной группе вычетов с нулевым умножением.

90. Доказать, что кольцо из четырех элементов 0, 1, a_1, a_2 с правилами действий $a_1^2=a_2$, $a_2^2=a_1$, $a_1a_2=a_2a_1=1$, $1+1=0$, $1+a_1=a_2$ образует поле.

91. Перечислить все кольца из четырех элементов, содержащие 0 и 1 (не предполагая ассоциативности и коммутативности).

92. Перечислить (с точностью до изоморфизма) конечные кольца с pq элементами, p и q — различные простые числа.

93. Пусть m — данное натуральное число. Рациональное число называется m-целым, если его знаменатель взаимно прост с m.

Доказать, что множество m-целых чисел образует кольцо (оно, очевидно, содержит кольцо целых чисел).

94. m-целое число называется обратимым или единицей, если обратное к нему тоже m-целое. m-целое число называется простым, если его нельзя представить в виде произведения двух m-целых необратимых чисел.

Доказать, что простыми m-целыми числами являются только простые делители числа m и произведения их на обратимые числа.

95. Доказать однозначность разложения m-целых чисел на простые множители.

96. Два m-целых числа называются сравнимыми по модулю m-целого числа k, если их разность делится на k в кольце m-целых чисел. Показать, что классы сравнимых по модулю k не изменятся, если заменить число k некоторым натуральным числом, состоящим только из простых делителей числа m.

97. Доказать обычные свойства сравнений для m-целых чисел: если $a_1 \equiv b_1 \pmod k$ и $a_2 \equiv b_2 \pmod k$, то $a_1+a_2 \equiv b_1+b_2$, $a_1-a_2 \equiv b_1-b_2$, $a_1a_2 \equiv b_1b_2 \pmod k$; если a и b — обратимы в кольце m-целых чисел и $a \equiv b \pmod k$, то $a^{-1} \equiv b^{-1} \pmod k$.

***98.** Найти наибольший общий делитель чисел a^m+b^m и a^n+b^n, в предположении взаимной простоты чисел a и b.

***99.** Доказать, что $1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1} \equiv 0 \pmod p$; здесь $p>2$ — простое число.

***100.** Доказать, что $1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1} \equiv 0 \pmod{p^2}$; здесь $p \geqslant 5$ — простое число.