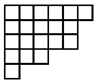
Элементы комбинаторики.

A1◇1. Сколько разных слов (не обязательно осмысленных) можно получить переставляя буквы в словах **а)** рок; **б)** урок; **в)** шнурок; **г)** курок; **д)** колобок; **е)** $\underbrace{\text{аа}\ldots\text{а}}_{a}\underbrace{\text{бб}\ldots\text{б}}_{b}$; **ж)** $\underbrace{б_1б_1\ldots б_1}_{k_1}\underbrace{б_2б_2\ldots б_2}_{k_2}\ldots\ldots\ldots\underbrace{б_mб_m\ldots б_m}_{k_m}$;.

A1◇2. Раскройте скобки и прведите подобные слагаемые в выражениях
а) $(a_1+a_2+\cdots+a_m)^2$; **б)** $(a+b+c)^3$; **в)** $(a+b)^n$; **г)** $(a_1+a_2+\cdots+a_m)^n$.

A1◇3. Фиксируем $m,n\in\mathbb{N}$. Сколько решений имеет уравнение $x_1+x_2+\cdots+x_m=n$
а) в натуральных **б)** в целых неотрицательных числах?

A1◇4. Сколько всего разных отображений из m-элементного множества в n-элементное?

A1◇5. Фигурка типа  (состоящая из выравненных по левому краю клетчатых горизонтальных полосок, длина которых невозрастает сверху вниз) называется *диаграммой Юнга*. Общее число клеток в диаграмме называется её *весом*. Сколько существует диаграмм Юнга
а) веса 6; **б)** веса 7, имеющих не более 3 строк;
в) произвольного веса, но имеющих не более p строк и не более q столбцов.

A1◇6. Имеются: 4 попарно отличающихся друг от друга чашки, 4 совершенно одинаковых гранёных стакана, 10 совершенно одинаковых кусков сахара и 7 попарно разноцветных соломинок. Сколькими способами можно разложить: **а)** соломинки по чашкам
б) сахар по чашкам **в)** сахар по стаканам **г)** соломинки по стаканам

A1◇7. Как изменятся ответы в предыдущей задаче, если потребовать, чтобы после раскладывания пустых ёмкостей не оставалось?

Мультиномиальные коэффициенты. Если $N=n_1+n_2+\cdots+n_\nu$ (все n_i – целые неотрицательные) то мы полагаем $\begin{pmatrix} N \\ n_1,n_2,\ldots,n_\nu\end{pmatrix}\overset{\text{def}}{=}\dfrac{N!}{n_1!\cdot n_2!\cdot\cdots\cdot n_\nu!}$. Такие числа называются *мультиномиальными коэффициентами*. При $\nu=2$ число $\begin{pmatrix} n \\ k,(n-k)\end{pmatrix}=\dfrac{n!}{k!(n-k)!}$ обозначается через $\binom{n}{k}$ и называется *биномиальным коэффициентом* или *числом сочетаний* из n по k. Отметим, что $\binom{n}{k}=\binom{n}{n-k}$. По определению, считается, что $\binom{n}{k}=0$ при $k,n<0$ и $k>n$, а также, что $\binom{n}{0}=\binom{n}{n}=1$ при всех $n\geqslant 0$.

A1◇8. Верно ли, что все мультиномиальные коэффициенты (скажем, $1000!/100!^{10}$) целые?

A1◇9. Вычислите: **а)** $\binom{n-1}{k-1}+\binom{n-1}{k}$; **б)** $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}$;
в) $\binom{k}{k}+\binom{k+1}{k}+\cdots+\binom{k+n}{k}$; **г*)** $\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2$.

A1◇10. Пусть p – простое число. Верно ли, что: **а)** $\binom{p}{k}$ либо равно 1 либо делится на p?
б*) $\binom{b_0+b_1p+\cdots+b_kp^k}{a_0+a_1p+\cdots+a_kp^k}\equiv\binom{b_0}{a_0}\binom{b_1}{a_1}\cdots\binom{b_k}{a_k} \mod p$?

A1◇11. При каких k $\binom{2p}{k}\not\equiv 0 \mod p$ для простого p?

Комплексные числа.

А2◇1. Вычислите (т. е. найдите вещественную и мнимые чати, модуль и аргумент):

а) $\dfrac{(5+i)(7-6i)}{3+i}$; **б)** $\dfrac{(1+i)^5}{(1-i)^3}$; **в)** $\left(\dfrac{\sqrt{3}+i}{1-i}\right)^{30}$; **г)** $(1+\cos\alpha+i\sin\alpha)^k$.

А2◇2. Решите уравнения: **а)** $z^2+(2i-7)z+(13-i)=0$; **б)** $z^3=i$;
в) $(z+1)^n-(z-1)^n=0$; **г)** $(z+i)^n+(z-i)^n=0$; **д)** $\overline{z}=z^3$.

А2◇3. Пусть $x=\cos\varphi$, $y=\sin\varphi$. Выразите $\operatorname{Re} z$, $\operatorname{Im} z$, $|z|$ и $Arg\, z$ числа $z=(x+iy)^n$ через φ; далее выразите: **а)** $\sin 5\varphi$ через $\sin\varphi$; **б)** $\cos\left({}^{2\pi}\!/_5\right)$ и $\sin\left({}^{4\pi}\!/_5\right)$ в радикалах.

А2◇4*. Пусть $m\in\mathbb{N}$ — нечётно. Убедитесь, что ${}^{\sin mx}\!/_{\sin x}$ является многочленом от $\sin^2 x$. Найдите его степень, корни и старший коэффициент. Справедливы ли тождества:

а) $\dfrac{\sin(mx)}{\sin\ x}=(-4)^{\frac{m-1}{2}}\prod\limits_{j=1}^{\frac{m-1}{2}}\left(\sin^2 x-\sin^2\left({}^{2\pi j}\!/_m\right)\right)$;

б) $(-1)^{\frac{m-1}{2}}\sin(mx)=2^{m-1}\prod\limits_{j=0}^{m-1}\sin\left(x+{}^{2\pi j}\!/_m\right)$.

А2◇5. Вычмслите z^m+1/z^m, если $z+1/z=2\cos\theta$.

А2◇6. Куда отображения $z\longmapsto z^2$ и $z\longmapsto 1/z$ переводят:
а) прямую $y=kx$; **б)** окружность $|z+i|=1$;
в) координатную сетку; **г)** кошечку с рис. 2.1 ?

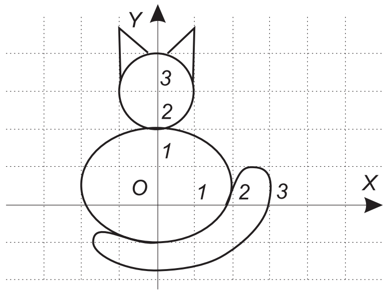


Рис. 2.1. Комплексная кошечка

А2◇7. Всегда ли вещественная и мнимая части корня квадратного уравнения с комплексными коэффициентами выражаются в радикалах через вещественные и мнимые части коэффициентов уравнения?

А2◇8. Вычислите сумму и произведение **а)** всех корней **б)** s-тых степеней всех корней степени n из 1.

А2◇9. Вычислите суммы: **а)** $\binom{n}{0}+\binom{n}{4}+\binom{n}{8}+\cdots$; **б)** $\binom{n}{1}+\binom{n}{5}+\binom{n}{9}+\cdots$;
в) $\binom{n}{1}-\dfrac{1}{3}\binom{n}{5}+\dfrac{1}{9}\binom{n}{9}+\cdots$; **г)** $\sin x+\sin 2x+\cdots+\sin nx$;
д) $\sin^2 x+\sin^2 3x+\cdots+\sin^2(2n-1)$; **е)** $\cos x+2\cos 2x+\cdots+n\cos nx$.

А2◇10. Верно ли, что попарно разные z_1, z_2, $z_3\in\mathbb{C}$ тогда и только тогда лежат на одной прямой, когда $\dfrac{z_1-z_3}{z_2-z_3}$ вещественно?

А2◇11. Верно ли, что четыре попарно разные точки z_1, z_2, z_3, $z_4\in\mathbb{C}$, не лежащие на одной прямой, тогда и только тогда лежат на одной окружности, когда их *двойное отношение* $\dfrac{(z_1-z_3):(z_2-z_3)}{(z_1-z_4):(z_2-z_4)}$ вещественно?

А2◇12. Докажите, что отображение $z\longmapsto(az+b)/(cz+d)$ (где $a,b,c,d\in\mathbb{C}$) переводит окружности и прямые или в окружности или в прямые, сохраняя при этом углы.

А2◇13. Верно ли, что всякое комплексное число $z\neq-1$ с $|z|=1$ можно представить в виде $z=\dfrac{1+ti}{1-ti}$ с $t\in\mathbb{R}$?

Элементы арифметики

(решение задач «со звёздочкой» скорее почётно, чем обязательно)

A3◇1 (алгоритм Евклида). Для любой пары натуральных чисел $A > B$ (соотв. многочленов A, B с $\deg A > \deg B$) положим $E_1 = A$, $E_2 = B$ и $E_\nu =$ остатку от деления $E_{\nu-2}$ на $E_{\nu-1}$ при $\nu = 3, 4, \dots$. Докажите, что последовательность E_ν (соотв. $\deg E_\nu$) строго монотонно убывает до тех пор, пока очередной $E_{\nu+1}$ не окажется нулевым и что последний ненулевой E_ν равен *НОД*(A, B), т. е. делит и A и B и делится на любой общий делитель A и B.

A3◇2. Докажите, что для любых целых чисел (соотв. многочленов) A, B можно подобрать такие целые числа (соотв. многочлены) a, b, что $aA + bB =$ *НОД*(A, B). Подберите такие a, b и вычислите *НОД*(A, B) для **а)** $A = 1537$, $B = 1387$; **б)** $A = x^5 - 1$, $B = x^4 + x^2 + 1$.

A3◇3. Пусть m – любой, а a, b – взаимно простые элементы произвольного кольца главных идеалов; верно ли, что

а) m делится на ab, если m делится и на a и на b;

б) a делит m, если a делит mb.

A3◇4. Верно ли, что $k \bmod n$ обратим в $\mathbb{Z}/n\mathbb{Z} \iff$ *НОД*$(n, k) = 1$ в $\mathbb{Z}$?

A3◇5. Составьте таблицы умножения для колец $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ и $\mathbb{Z}/8\mathbb{Z}$. В каждом из этих колец найдите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты. Для обратимых элементов постройте таблицу обратных.

Редукция по модулю n — это гомоморфизм $\mathbb{Z} \xrightarrow{res_n} \mathbb{Z}/n\mathbb{Z}$, переводящий $m \in \mathbb{Z}$ в класс вычетов $m \bmod n$. Применяя его к уравнению в кольце $\mathbb{Z}$, мы получаем уравнение в кольце $\mathbb{Z}/n\mathbb{Z}$, неразрешимость которого влечёт, очевидно, неразрешимость исходного уравнения. Поскольку $\mathbb{Z}/n\mathbb{Z}$ конечно, редукции по подходящему модулю иногда резко упрощает анализ разрешимости.

A3◇6. Докажите, что уравнение $15x^2 - 7y^2 = 9$ не имеет решений в целых числах.

A3◇7. Найдите все целые решения уравнений $x^2 + y^2 + z^2 = 2xyz$ и $5x^3 + 11y^3 + 13z^3 = 0$.

A3◇8. Пусть p – простое число. Будет ли $\mathbb{Z}/p\mathbb{Z}$ полем? Найдите все $x \in \mathbb{Z}/p\mathbb{Z}$, такие что $x^2 = 1$, и вычислите произведение всех ненулевых чисел в $\mathbb{Z}/p\mathbb{Z}$.

A3◇9 (теорема Вильсона). Докажите, что натуральное $p \geqslant 2$ является простым тогда и только тогда, когда $(p-1)! + 1 \equiv 0 \pmod p$.

A3◇10 (малая теорема Ферма). Докажите, что для любого целого числа m, не делящегося на простое число p, выполнено сравнение $m^{p-1} \equiv 1 \mod p$.

A3◇11. Пусть p – простое число. Выясните, сколько всего ненулевых квадратов в $\mathbb{Z}/p\mathbb{Z}$ и всегда ли в $\mathbb{Z}/p\mathbb{Z}$ разрешимо уравнение $x^2 + y^2 = -1$.

A3◇12. Выясните, являются ли следующие ниже два кольца евклидовыми относительно высоты $\lambda(z) = |z|^2$ и найдите в них все обратимые элементы

а) *гауссовы целые числа* $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{\, a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z} \,\}$

б) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z}\,,\ \omega^2 + \omega + 1 = 0\,\}$

A3◇13*. Разложите 5 на простые множители в кольце $\mathbb{Z}[i]$. Какие простые $p \in \mathbb{Z}$ остаются простыми и в $\mathbb{Z}[i]$?

Квадратичная взаимность

А$3\frac{1}{2}\diamond$1. Какие значения может принимать функция $y = x^{(p-1)/2}$ на ненулевых элементах $\mathbb{Z}/p\mathbb{Z}$ при простом p? Верно ли, что ненулевой $x \in \mathbb{Z}/p\mathbb{Z}$ тогда и только тогда является квадратом, когда $x^{(p-1)/2} = 1$?

А$3\frac{1}{2}\diamond$2 (лемма Гаусса). Пусть $p \in \mathbb{N}$ — простое. Выпишем все элементы поля $\mathbb{Z}/p\mathbb{Z}$ подряд в виде: $-{(p-1)}/{2}\,,\ \dots\,,\ -1\,,\ 0\,,\ 1\,,\ \dots\,,\ {(p-1)}/{2}$. Докажите, что

а) a тогда и только тогда квадрат в $\mathbb{Z}/p\mathbb{Z}$, когда в предыдущей записи чётное число положительных чисел меняет знак при умножении на a;

б) -1 квадрат в $\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда, когда $p \equiv 1 \pmod 4$ или $p = 2$;

в) 2 квадрат в $\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда, когда $(p^2-1)/8$ чётно.

Символ Лежандра - Якоби. Пусть p – простое число. Сопоставим каждому $n \in \mathbb{Z}$ число

$$\left(\frac{n}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 0\,, \text{если } n \text{ делится на } p\,, \\ 1\,, \text{если } n \bmod p \text{ ненулевой квадрат в } \mathbb{Z}/p\mathbb{Z}\,, \\ -1\,, \text{если } n \bmod p \text{ не квадрат в } \mathbb{Z}/p\mathbb{Z}\,. \end{cases}$$

А$3\frac{1}{2}\diamond$3. Докажите, что при фиксированном p символ $\left(\frac{n}{p}\right)$ представляет собой мультипликативный характер[1] числа n и что $\displaystyle\sum_{n=1}^{p-1}\left(\frac{n}{p}\right) = 0$.

А$3\frac{1}{2}\diamond$4*. Совпадают ли знаки у $\left(\frac{m}{p}\right)$ и $\displaystyle\prod_{j=1}^{(p-1)/2}\frac{\sin\left(m\cdot 2\pi j/p\right)}{\sin\left(2\pi j/p\right)}$?

А$3\frac{1}{2}\diamond$5* (квадратичный закон взаимности). Докажите, что для любых простых чисел p, q

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

Указание. Примените зад. А$3\frac{1}{2}\diamond$4, разложив все отношения синусов по формулам из зад. А$2\diamond$4.

А$3\frac{1}{2}\diamond$6*. Найдите $\left(\frac{43}{109}\right)$.

А$3\frac{1}{2}\diamond$7*. Докажите, что следующие условия на простое число $p \in \mathbb{Z}$ попарно равносильны:

а) p перестаёт быть простым в $\mathbb{Z}[i]$;

б) p является суммой двух квадратов натуральных чисел;

в) -1 является квадратом в $\mathbb{Z}/p\mathbb{Z}$;

г) $p \not\equiv 3 \mod 4$.

А$3\frac{1}{2}\diamond$8* (разложение в сумму двух квадратов). Верно ли, что натуральное число тогда и только тогда не является ни квадратом ни суммой двух натуральных квадратов, когда в его разложении на простые множители входит нечётная степень простого числа вида $4k+3$.

Указание. Воспользуйтесь предыдущей задачей, факториальностью колец $\mathbb{Z}$ и $\mathbb{Z}[i]$ и тем, что равенство $m = a^2+b^2$ в кольце $\mathbb{Z}$ равносильно равенству $m = (a+ib)(a-ib) = z\overline{z}$ в кольце $\mathbb{Z}[i]$.

---

[1] функция $\mathbb{Z} \xrightarrow{f} \mathbb{C}$ называется *мультипликативным характером*, если $f(mn) = f(m)f(n)$ всякий раз, когда *НОД*$(m,n) = 1$; применительно к символу Лежандра - Якоби это означает, что $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\cdot\left(\frac{n}{p}\right)$ для взаимно простых m, n

Коммутативные кольца, гомоморфизмы и идеалы

A4◇1. Пусть $A \xrightarrow{\varphi} B$ – ненулевой гомоморфизм коммутативных колец с единицами. Верно ли, что $\varphi(1) = 1$? А если в B нет делителей нуля?

A4◇2. Найдите: **а)** все автоморфизмы поля $\mathbb{C}$, оставляющие на месте каждый элемент из $\mathbb{R}$, **б)** все автоморфизмы поля $\mathbb{Q}(\sqrt[3]{2}) \stackrel{\text{def}}{=} \mathbb{Q}[x]/(x^3-2)$.

A4◇3°. Верно ли, что коммутативное кольцо с 1 является полем тогда и только тогда, когда оно не имеет идеалов, отличных от (0) и всего кольца?

A4◇4 (китайская теорема об остатках). Известно, что натуральные числа $\{n_1, n_2, \dots, n_s\}$ попарно взаимно просты, а их произведение равно n. Постройте изоморфизм кольца $\mathbb{Z}/n\mathbb{Z}$ с прямой суммой колец $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/n_s\mathbb{Z}$. Опишите все натуральные числа с остатками 1, 2, 3 от деления, соответственно, на 5, 6 и 7.

A4◇5. Сформулируйте и докажите аналог предыдущей задачи для кольца многочленов с коэффициентами в произвольном поле. Опишите все многочлены $f \in \mathbb{Q}[x]$, имеющие остатки $1+x$, $1+x^3$ и $1+x^5$ от деления на $1+x^2$, $1+x^4$ и $1+x^8$ соответственно.

A4◇6. Решите в $\mathbb{Z}/360\mathbb{Z}$ уравнения **а)** $x^2 = 1$ **б)** $x^3 = 1$ **в)** $x^2 = 49$.

A4◇7. Являются ли $\mathbb{Q}[x, y]$ и $\mathbb{Z}[x]$ кольцами главных идеалов?

Простота, максимальность и неприводимость. Идеал $\mathfrak{a} \subset A$ называется *простым* (соотв. *максимальным*), если $A/\mathfrak{a}$ не имеет делителей нуля (соотв. является полем). Отметим, что максимальные идеалы, очевидно, просты. Элемент $a \in A$ называется *простым*, если идеал (a) прост. Элемент кольца называется *неприводимым*, если он не является произведением двух необратимых элементов.

A4◇8. Опишите все идеалы и все максимальные идеалы кольца формальных степенных рядов $k[[x]]$ над полем k.

A4◇9. Равносильна ли простота элемента p тому, что $\forall\, a, b \quad p|ab \;\Rightarrow\; p|a$ или $p|b$?

A4◇10. Докажите, что максимальные идеалы просты, а простые элементы неприводимы.

A4◇11. Найдите в кольце $\mathbb{Z}[\sqrt{5}]$ непростой неприводимый элемент.

A4◇12. Верно ли, что в любом целостном кольце главных идеалов:

а) простота элемента равносильна его неприводимости ;

б) $\forall$ цепочки вложенных идеалов $I_1 \subset I_2 \subset \cdots \; \exists\, n : I_\nu = I_{\nu+1}$ при $\nu \geqslant n$;

в) любой элемент раскладывается в произведение конечного числа неприводимых;

г) справедлива теорема об однозначности разложения на неприводимые множители?

A4◇13. Пусть $f, g \in \mathbb{Z}[x]$ не имеют общих делителей, отличных от ± 1. Конечно ли фактор-кольцо $\mathbb{Z}[x]/(f, g)$?

A4◇14°. Докажите, что идеал максимален тогда и только тогда, когда он не содержится ни в каком строго большем идеале, отличном от всего кольца.

A4◇15. Будет ли полем $\mathbb{R}[x]/(f(x))$, если **а)** $f = x^4 + 1$, **б)** $f = x^3 + 1$, **в)** $f = x^2 + 3$?

A4◇16. Обозначим поле $\mathbb{Z}/p\mathbb{Z}$, где p — простое, через $\mathbb{F}_p$, и пусть $f \in \mathbb{F}_p[x]$ — неприводимый многочлен степени n. Сколько элементов в факторе $\mathbb{F}_p[x]/(f)$? Является ли он полем?

A4◇17. Пусть k — любое (возможно, конечное) поле. Бесконечно ли множество неприводимых многочленов в $k[x]$? Есть ли ограничения на степени неприводимых многочленов?

A4◇18*. Есть ли среди фактор колец кольца $\mathbb{Z}[i]$ поле характеристики **а)** 2 **б)** 3, и если да, то сколько в нём может быть элементов?

A4◇19*. При каком простом p существует нентривиальный гомомрфизм $\mathbb{Z}[i] \longrightarrow \mathbb{Z}/p\mathbb{Z}$?

Примеры на делимость

А$4\frac{1}{2}\diamond$1. В кольце $\mathbb{Z}[x]$ разложите на неприводимые множители или докажите неприводимость многочленов: **а)** t^4+t+1, **б)** $t^5+t^4+t^2+t+2$, **в)** t^6+t^3+1, **г)** $x^{p-1}+\ldots+x+1$ при простом $p>1$.

Функция Эйлера. Для каждого $n\in\mathbb{Z}$ обозначим через $\varphi(n)$ *функцию Эйлера* — число обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$ (т. е. количество всех взаимно простых с n чисел $k\in\mathbb{N}$, не превосходящих $n-1$).

А$4\frac{1}{2}\diamond$2. Проверьте, что функция Эйлера является мультипликативным характером, и что если $m=p_1^{k_1}\cdot\ldots\cdot p_n^{k_n}$ — разложение на простые множители, то

а) $\varphi(m)=\varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_n^{k_n})$; **б)** $\varphi(m)=m\cdot\left(1-\dfrac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\dfrac{1}{p_n}\right)$.

А$4\frac{1}{2}\diamond$3. Найдите все m такие, что $\varphi(m)=10$.

А$4\frac{1}{2}\diamond$4 (теорема Эйлера). Выясните, чему равно произведение всех обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$ и вычислите $a^{\varphi(m)}$ для данного обратимого $a\in\mathbb{Z}/n\mathbb{Z}$.

Функция Мёбиуса. Пусть $m\in\mathbb{Z}$ разложено на простые множители: $m=p_1^{k_1}\cdot\ldots\cdot p_n^{k_n}$; значение *функции Мёбиуса* $\mu(m)$ на числе m по определению равно 0, если хоть один из показателей $k_i\geqslant 2$ (т. е. если m делится на ненулевой квадрат), и равно $(-1)^n$, если все показатели $k_1,k_2,\ldots,k_n$ равны 1. В частности, при $m=0$ имеем $\mu(1)\overset{\text{def}}{=}1$.

А$4\frac{1}{2}\diamond$5. Убедитесь, что $\mu(m)$ является мультипликативным характером, и докажите тождество
$$\sum_{d|n}\mu(d)=\begin{cases}1, & \text{при } n=1\\ 0, & \text{при } n>1\end{cases}.$$

А$4\frac{1}{2}\diamond$6 (обращение Мёбиуса). Пусть для функции $\mathbb{N}\xrightarrow{g}\mathbb{C}$ при каждом $n\in\mathbb{N}$ известно значение суммы $\sigma(n)=\sum\limits_{d|n}g(d)$. Докажите, что тогда функцию g можно восстановить по функции σ при помощи формулы $g(n)=\sum\limits_{d|n}\mu(n/d)\sigma(d)$.

А$4\frac{1}{2}\diamond$7. Для данного $m\in\mathbb{N}$ вычислите $\sum\limits_{d|m}\varphi(d)$.

Круговые многочлены. Комплексное число $\zeta\in\mathbb{C}$ называется *первообразным корнем n-той степени*, если все комплексные решения уравнеия $z^n=1$ являются степенями ζ. Многочлен $f_n(x)\overset{\text{def}}{=}\prod\limits_{\zeta}(x-\zeta)\in\mathbb{C}[x]$, где ζ пробегает все различные первообразные корни степени n, называется *n-тым круговым многочленом*.

А$4\frac{1}{2}\diamond$8. Для любого ли $n\in\mathbb{N}$ существуют первообразные корни n-той степени?

А$4\frac{1}{2}\diamond$9. Правда ли, что $x^n-1=\prod\limits_{d|n}f_d(x)$? Используя подходящую модификацию обращения Мёбиуса, докажите, что $f_n(x)=\prod\limits_{d|n}(x^{n/d}-1)^{\mu(d)}$.

А$4\frac{1}{2}\diamond$10. Докажите, что при всех $n\in\mathbb{N}$ n-тый круговой многочлен f_n имеет степень $\varphi(n)$, целые коэффициенты и неприводим над $\mathbb{Z}$.

А$4\frac{1}{2}\diamond$11. Пусть $p\in\mathbb{N}$ – простое. Верно ли, что: **а)** $f_{2n}(x)=f_n(-x)$ при нечётном n; **б)** $f_p(x)=x^{p-1}+\cdots+x+1$; **в)** $f_{p^k}(x)=f_p\left(x^{p^{k-1}}\right)$ **г)** $f_{pm}(x)=\dfrac{f_m(x^p)}{f_m(x)}$ при $p\nmid m$.

А$4\frac{1}{2}\diamond$12. Докажите, что если $m=p_1^{k_1}\cdot\ldots\cdot p_n^{k_n}$ (p_i — различные простые числа), то
$$f_m(x)=f_{p_1p_2\cdots p_n}\left(x^{p_1^{k_1-1}\cdots p_n^{k_n-1}}\right).$$

Первообразные корни в кольце вычетов. Пусть a – обратимый элемент кольца $\mathbb{Z}/n\mathbb{Z}$. Назовём *порядком* вычета a наименьшее натуральное число k такое, что $a^k = 1$. Элемент a называется *первообразным корнем по модулю* n , если все прочие обратимые вычеты являются его степенями.

A4$\frac{1}{2}\diamond$13. Пусть порядки $k_1, k_2, \dots, k_n$ вычетов $a_1, a_2, \dots, a_n$ попарно взаимно просты. Чему равен порядок вычета $a = a_1 \cdot \dots \cdot a_n$?

A4$\frac{1}{2}\diamond$14. Пусть вычеты порядков k и l существуют. Существует ли вычет порядка $HOK(k, l)$?

A4$\frac{1}{2}\diamond$15. Докажите, что для существования первообразного корня необходимо и достаточно существование обратимого вычета порядка $\varphi(n)$. По любому ли простому модулю существует первообразный корень?

A4$\frac{1}{2}\diamond$16*. Пусть ϱ — первообразный корень по простому модулю $p > 2$. Докажите, что существует $\vartheta \in \mathbb{N}$, такое что $(\varrho + p\vartheta)^{p-1} \equiv 1 \mod p$, но $(\varrho + p\vartheta)^{p-1} \not\equiv 1 \mod p^2$. Верно ли, что класс $\varrho + p\vartheta$ является первообразным корнем по модулю p^k для всех $k \in \mathbb{N}$?

A4$\frac{1}{2}\diamond$17*. Докажите существование первообразного корня $\mathrm{mod}\, 2\, p^k$ $\forall\, k \in \mathbb{N}$ и простого p.

A4$\frac{1}{2}\diamond$18. Существует ли первообразный корень по модулю 21?

Комбинаторика обращения Мёбиуса

чумы. Множество $\mathfrak{P}$, для *некоторых* пар элементов которого задано отношение порядка $\leqslant$ со свойствами:

$$(1) \quad (x \leqslant y \quad \& \quad y \leqslant x) \Leftrightarrow (x = y); \qquad\qquad (2) \quad (x \leqslant y \quad \& \quad y \leqslant z) \Rightarrow (x \leqslant z)\ .$$

частично упорядоченным множеством (сокращённо чумом). чум называется *локально конечным*, если для всех $x, y \in \mathfrak{P} \times \mathfrak{P}$ множество $[x, y] \stackrel{\text{def}}{=} \{\, z \mid x \leqslant z \leqslant y \,\}$ – конечно. Множество функций $\varrho(x, y)$: $\mathfrak{P} \times \mathfrak{P} \longrightarrow \mathbb{C}$, удовлетворяющих условию $\varrho(x, y) = 0$ при $x > y$, с операциями

$$[\varrho_1 + \varrho_2]\,(x, y) \stackrel{\text{def}}{=} \varrho_1(x, y) + \varrho_2(x, y) \qquad \text{и} \qquad [\varrho_1 \star \varrho_2]\,(x, y) \stackrel{\text{def}}{=} \sum_{x \leqslant z \leqslant y} r_1(x, z) r_2(z, y)$$

называется *агеброй инцидентности* чума $\mathfrak{P}$ и обозначается через $\mathcal{A}(\mathfrak{P}\,)$.

A4$\frac{1}{2}\diamond$19. Будет ли локально конечным чумом множество: **а)** $\mathbb{Z}$ с отношением $n|m$.
б) конечных подмножеств данного множества с отношением $X \subseteq Y$;
в) вершин ориентированного графа ($x \leqslant y$ если имеется ориентированный путь из x в y);

A4$\frac{1}{2}\diamond$20. Проверьте, что $\mathcal{A}(\mathfrak{P}\,)$ является (некоммутативным) кольцом с единицей и докажите, что $\varrho(x, y) \in \mathcal{A}(\mathfrak{P}\,)$ обратим тогда и только тогда, когда $\varrho(x, x) \neq 0 \quad \forall\, x \in \mathfrak{P}$.

Обращение Мёбиуса. Функция $\zeta(x, y) \stackrel{\text{def}}{=} \begin{cases} 1\,, & \text{при} \quad x \leqslant y \\ 0\,, & \text{при} \quad x > y \end{cases}$ называется *функцией инцидентности* (или ζ-*функцией*), а функция $\mu(x, y)$, обратная к $\zeta(x, y)$ в $\mathcal{A}(\mathfrak{P}\,)$, — *функцией Мебиуса* чума $\mathfrak{P}$.

A4$\frac{1}{2}\diamond$21. Докажите равенства: **а)** $\mu(x, y) = -\sum\limits_{x \leqslant z < y} \mu(x, z)$; **б)** $\mu(x, y) = -\sum\limits_{x < z \leqslant y} \mu(z, y)$.

A4$\frac{1}{2}\diamond$22. Постройте функцию Мебиуса для $\mathbb{Z}$ с отношением $x|y$, для множества всех подмножеств данного n-элементного множества и для ориентированного дерева.

A4$\frac{1}{2}\diamond$23 (формула обращения). Пусть для функции $\mathfrak{P} \xrightarrow{\ g\ } \mathbb{C}$ известны значения всех сумм $\sigma(x) = \sum\limits_{y<x} g(y)$. Верно ли, что g восстанавливается из σ по формуле $g(x) = \sum\limits_{y<x} \sigma(y)\mu(y, x)$?