Обращение Мёбиуса

Функция Мёбиуса $\mu(n)$ сопоставляет каждому $n\in\mathbb{N}$ нуль, если n делится на квадрат простого числа, и $(-1)^s$, где s — число всех натуральных простых делителей n, если n не делится на квадраты простых чисел; кроме того, $\mu(1)\stackrel{\text{def}}{=}1$.

А$3\frac{1}{2}$◇1. Верно ли, что $\mu(m)$ — мультипликативный характер и $\sum\limits_{d|n}\mu(d)=\begin{cases}1\,, & \text{при}\quad n=1\\ 0\,, & \text{при}\quad n>1\end{cases}$?

А$3\frac{1}{2}$◇2 (обращение Мёбиуса). Пусть для функции $\mathbb{N}\xrightarrow{\ g\ }\mathbb{C}$ при каждом $n\in\mathbb{N}$ известно значение суммы $\sigma(n)=\sum\limits_{d|n}g(d)$. Покажите, что функция g восстанавливается по функции σ по формуле $g(n)=\sum\limits_{d|n}\mu(n/d)\sigma(d)$.

А$3\frac{1}{2}$◇3. Для произвольного $m\in\mathbb{N}$ вычислите $\sum\limits_{d|m}\varphi(d)$, где φ — функция Эйлера.

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

А$3\frac{1}{2}$◇4. Для любого ли $n\in\mathbb{N}$ существуют первообразные корни n-той степени?

А$3\frac{1}{2}$◇5. 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$3\frac{1}{2}$◇6. Покажите, что $f_n\in\mathbb{Z}[x]$ и найдите $\deg f_n$. Приводим ли f_n над $\mathbb{Z}$?

А$3\frac{1}{2}$◇7. Пусть $p\in\mathbb{N}$ — простое. Докажите тождества: **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)** $f_{pm}(x)=\dfrac{f_m\left(x^p\right)}{f_m(x)}$ при $p\nmid m$.

д) $f_{p_1^{k_1}\cdots p_n^{k_n}}(x)=f_{p_1p_2\cdots p_n}\left(x^{p_1^{k_1-1}\cdots p_n^{k_n-1}}\right)$, где все p_i просты и различны.

Конечные поля. Обозначим через $\mathbb{F}_q$ произвольное поле из q элементов, а через $\mathbb{F}_q^*$ — мультипликативную группу всех его ненулевых элементов.

А$3\frac{1}{2}$◇8. Образуют ли поле корни многочлена $x^{p^k}-x$ в произвольном поле характеристики p?

А$3\frac{1}{2}$◇9. Докажите, что порядок любого $\zeta\in\mathbb{F}_q^*$ делит $q-1$ и, пользуясь обращением Мёбиуса, напишите формулу для числа элементов d-того порядка.

А$3\frac{1}{2}$◇10. Докажите, что группа $\mathbb{F}_q^*$ — циклическая, и выясните, сколько в ней элементов $(q-1)$-го порядка.

А$3\frac{1}{2}$◇11. Какова степень минимального могочлена элемента $(q-1)$-го порядка в $\mathbb{F}_{p^n}^*$ над $\mathbb{F}_p$?

А$3\frac{1}{2}$◇12 (гомоморфизм Фробениуса). Будет ли отображение $x\mapsto x^p$ гомоморфизмом в произвольном поле характеристики p? Как оно действует на простом подполе?

А$3\frac{1}{2}$◇13 (описание конечных полей). Докажите, что число элементов в любом конечном поле k является степенью простого числа $p=char(k)$ и что для любого простого p и натурального n поле $\mathbb{F}_q$ из $q=p^n$ элементов существует и единственно с точностью до изоморфизма.

А$3\frac{1}{2}$◇14. При каких q_1, q_2 существует ненулевой гомоморфизм $\mathbb{F}_{q_1}\longrightarrow\mathbb{F}_{q_2}$? Опишите все автоморфизмы поля из p^n элементов.

А$3\frac{1}{2}$◇15*. Чему равна наибольшая из степеней неприводимых делителей многочлена $x^{p^k}-x$ над $\mathbb{F}_p$? Как этот многочлен раскладывается на множители?

А$3\frac{1}{2}$◇16*. Обозначим через i_m число всех неприводимых над $\mathbb{F}_p$ многочленов степени m со старшим коэффициентом 1. Верно ли, что $(1-pz)^{-1}=\prod\limits_{m\in\mathbb{N}}(1-z^m)^{-i_m}$ в $\mathbb{Q}[[z]]$? Используя

надлежащую версию обращения Мёбиуса, докажите, что число неприводимых над $\mathbb{F}_p$ многочленов степени n равно $\bigl({}^{1}\!/_{n}\bigr)\cdot\sum\limits_{d|n}\mu\bigl({}^{n}\!/_{d}\bigr)\,p^d$.

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.

А3$\frac{1}{2}\diamond$17. Пусть порядки $k_1,k_2,\ldots,k_n$ вычетов $a_1,a_2,\ldots,a_n$ попарно взаимно просты. Чему равен порядок вычета $a=a_1\cdots a_n$?

А3$\frac{1}{2}\diamond$18. Пусть вычеты порядков k и l существуют. Существует ли вычет порядка $\text{нок}(k,l)$?

А3$\frac{1}{2}\diamond$19. Докажите, что для существования первообразного корня необходимо и достаточно существование обратимого вычета порядка $\varphi(n)$. По любому ли простому модулю существует первообразный корень?

А3$\frac{1}{2}\diamond$20*. Пусть ϱ — первообразный корень по простому модулю $p>2$. Докажите, что существует $\vartheta\in\mathbb{N}$, такое что $(\varrho+p\vartheta)^{p-1}\equiv 1\,(\mathrm{mod}\,p)$, но $(\varrho+p\vartheta)^{p-1}\not\equiv 1\,(\mathrm{mod}\,p^2)$. Верно ли, что класс $\varrho+p\vartheta$ является первообразным корнем по модулю p^k для всех $k\in\mathbb{N}$?

А3$\frac{1}{2}\diamond$21*. Докажите существование первообразного корня $\mathrm{mod}\,2\,p^k\ \ \forall\,k\in\mathbb{N}$ и простого p.

А3$\frac{1}{2}\diamond$22. Существует ли первообразный корень по модулю 21?

Комбинаторика обращени Мёбиуса. Множество $\mathfrak{P}$, для *некоторых* пар элементов которого задано отношение $\leqslant$ со свойствами: $(x\leqslant y\ \ \&\ \ y\leqslant x)\Leftrightarrow(x=y)$ и $(x\leqslant y\ \ \&\ \ y\leqslant z)\Rightarrow(x\leqslant z)$ называется *частично упорядоченным множеством* (сокращённо чумом). чум *локально конечен*, если для всех $x,y\in\mathfrak{P}\times\mathfrak{P}$ множество $[x,y]\overset{\text{def}}{=}\{\,z\mid x\leqslant z\leqslant y\,\}$ — конечно. Множество функций $\varrho(x,y):\mathfrak{P}\times\mathfrak{P}\longrightarrow\mathbb{C}$, которые могут принимать ненулевые значения *только* при $x\leqslant y$, с операциями

$$[\varrho_1+\varrho_2]\,(x,y)\overset{\text{def}}{=}\varrho_1(x,y)+\varrho_2(x,y)\qquad\text{и}\qquad[\varrho_1*\varrho_2]\,(x,y)\overset{\text{def}}{=}\sum_{x\leqslant z\leqslant y}\varrho_1(x,z)\varrho_2(z,y)$$

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

$$\zeta(x,y)\overset{\text{def}}{=}\begin{cases}1 & \text{при}\quad x\leqslant y\,,\\ 0 & \text{в остальных случаях}\end{cases}$$

называется *функцией инцидентности*, а функция $\mu(x,y)$, обратная к $\zeta(x,y)$ в кольце $\mathscr{A}(\mathfrak{P})$, называется *функцией Мебиуса* чума $\mathfrak{P}$.

А3$\frac{1}{2}\diamond$23. Являются ли локально конечными чумами: **а)** множество $\mathbb{N}$ с отношением $n|m$.

б) множество конечных подмножеств произвольного множества с отношением $X\subseteq Y$;

в) множество вершин ориентированного графа без ориентированных петель с отношением $x\leqslant y\Longleftrightarrow$ имеется ориентированный путь из x в y.

А3$\frac{1}{2}\diamond$24. Проверьте, что $\mathscr{A}(\mathfrak{P})$ является (некоммутативным) кольцом с единицей и докажите, что $\varrho(x,y)\in\mathscr{A}(\mathfrak{P})$ обратим (с обеих сторон) тогда и только тогда, когда $\forall\,x\in\mathfrak{P}\ \ \varrho(x,x)\neq 0$ (в частности, функция инцдентности на самом деле обратима).

А3$\frac{1}{2}\diamond$25. Докажите равенства[1]: **а)** $\mu(x,y)=-\sum\limits_{x\leqslant z<y}\mu(x,z)$; **б)** $\mu(x,y)=-\sum\limits_{x<z\leqslant y}\mu(z,y)$.

А3$\frac{1}{2}\diamond$26 (обращение Мёбиуса). 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 $g(x)=\sum\limits_{y<x}\sigma(y)\mu(y,x)$?

А3$\frac{1}{2}\diamond$27. Постройте функцию Мебиуса для $\mathbb{N}$ с отношением $x|y$ и для подмножеств данного n-элементного множества с отношением $X\subset Y$. Как выглядят для них формулы обращения?

[1] условимся писать $x<y$, когда $x\leqslant y$ и $x\neq y$