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, положим $\mu(1) = 1$. Всюду далее запись $d|N$ означает: «d нацело делит m».

A$6\frac{1}{2}$◇1. Является ли функция $\mu(m)$ мультипликативным характером[1]?

A$6\frac{1}{2}$◇2. Вычислите $\sum\limits_{d|n} \mu(d)$ при $n > 1$ (отметим, что при $n = 1$ эта сумма очевидно равна 1).

A$6\frac{1}{2}$◇3 (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 функция g восстанавливается по функции σ по формуле $g(n) = \sum\limits_{d|n} \mu(n/d)\sigma(d)$.

A$6\frac{1}{2}$◇4. 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 $f_n(x) = \prod(x - \zeta) \in \mathbb{C}[x]$, где ζ пробегает все различные первообразные корни степени n, называется n-тым *круговым*[2] *многочленом*.

A$6\frac{1}{2}$◇5. Для любого ли $n \in \mathbb{N}$ существуют первообразные корни n-той степени?

A$6\frac{1}{2}$◇6. Докажите, что $x^n - 1 = \prod\limits_{d|n} f_d(x)$, и, используя подходящую модификацию обращения Мёбиуса, выведите из этого, что $f_n(x) = \prod\limits_{d|n} (x^{n/d} - 1)^{\mu(d)}$.

A$6\frac{1}{2}$◇7. Покажите, что $f_n \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$ и $\deg f_n = \varphi(n)$.

A$6\frac{1}{2}$◇8. 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)** $f_{pm}(x) = \dfrac{f_m(x^p)}{f_m(x)}$ при $p \nmid m$. **д)** $f_{p_1^{k_1} \cdots p_n^{k_n}}(x) = f_{p_1 p_2 \cdots p_n}\left(x^{p_1^{k_1-1} \cdots p_n^{k_n-1}}\right)$, 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.

A$6\frac{1}{2}$◇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.

A$6\frac{1}{2}$◇10. Покажите, что $\mathbb{F}_q^*$ является циклической группой, и выясните сколько в ней имеется элементов $(q - 1)$-го порядка.

A$6\frac{1}{2}$◇11. Рассмотрим в произвольном поле характеристики p все корни многочлена $x^{p^k} - x$. Образуют ли они поле?

A$6\frac{1}{2}$◇12. Какова степень минимального многочлена над $\mathbb{Z}/(p)$ элемента $(q - 1)$-го порядка в $\mathbb{F}_{p^n}^*$?

A$6\frac{1}{2}$◇13. Покажите, что число элементов q конечного поля $\mathbb{F}_q$ является некоторой натуральной степенью характеристики p этого поля.

A$6\frac{1}{2}$◇14. Докажите, что для любого простого p и натурального n существует единственное с точностью до изоморфизма поле $\mathbb{F}_q$ из $q = p^n$ элементов.

A$6\frac{1}{2}$◇15. 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.

---

[1] функция $\mathbb{N} \xrightarrow{f} \mathbb{C}$ называется *мультипликативным характером*, если для любых взаимно простых $m, n \in \mathbb{N}$ выполняется соотношение $f(mn) = f(m)f(n)$

[2] или *циклотомическим*

A$6\frac{1}{2}$◇16*. Чему равна наибольшая из степеней неприводимых делителей многочлена $x^{p^k}-x$ над $\mathbb{Z}/(p)$? Как он раскладывается на множители?

A$6\frac{1}{2}$◇17*. Обозначим через i_m число всех неприводимых над $\mathbb{Z}/(p)$ 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 $\mathbb{Z}/(p)$ многочленов степени n равно $\left(1/n\right)\cdot\sum\limits_{d|n}\mu\left(n/d\right)p^d$.

Комбинаторика обращени Мёбиуса. Множество $\mathfrak{P}$, для *некоторых* пар элементов которого задано отношение $\leqslant$ со свойствами: $(x\leqslant y \quad \& \quad y\leqslant x)\Leftrightarrow(x=y)$ и $(x\leqslant y \quad \& \quad y\leqslant z)\Rightarrow(x\leqslant z)$ 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 $\mathfrak{P}$.

A$6\frac{1}{2}$◇18. 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 $x\leqslant y\iff$ имеется ориентированный путь из x в y.

A$6\frac{1}{2}$◇19. 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 $\forall\,x\in\mathfrak{P}\quad\varrho(x,x)\neq0$ (в частности, функция инцдентности на самом деле обратима).

A$6\frac{1}{2}$◇20. Докажите равенства[3]: **а)** $\mu(x,y)=-\sum\limits_{x\leqslant z<y}\mu(x,z)$; **б)** $\mu(x,y)=-\sum\limits_{x<z\leqslant y}\mu(z,y)$.

A$6\frac{1}{2}$◇21 (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 $g(x)=\sum\limits_{y<x}\sigma(y)\mu(y,x)$?

A$6\frac{1}{2}$◇22. 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?

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