Обращение Мёбиуса

А3½◇1 (арифметическая функция Мёбиуса). Функция Мёбиуса $\mu : \mathbb{N} \to \mathbb{N} \cup \{0\}$ переводит n в 0, если n делится на квадрат простого числа, и в $(-1)^s$, где s — число натуральных простых делителей n, если n не делится на квадраты простых чисел; кроме того, $\mu(1) \stackrel{\text{def}}{=} 1$. Покажите, что **а)** $\mu(mn) = \mu(m)\mu(n)$ если НОД$(m, n) = 1$ **б)** $\sum\limits_{d|n} \mu(d) = \begin{cases} 1 \text{ при } n = 1 \\ 0 \text{ при } n > 1. \end{cases}$

А3½◇2 (арифметическое обращение Мёбиуса). Пусть для функции $g : \mathbb{N} \to \mathbb{C}$ при каждом $n \in \mathbb{N}$ известно значение суммы $\sigma(n) = \sum_{d|n} g(d)$. Покажите, что $g(n) = \sum_{d|n} \sigma(d) \cdot \mu(n/d)$.

А3½◇3. Для произвольного $m \in \mathbb{N}$ вычислите $\sum_{d|m} \varphi(d)$, где φ — функция Эйлера.

А3½◇4 (круговые многочлены). Приведённый многочлен $\Phi_n \in \mathbb{C}[x]$, корни которого суть комплексные первообразные корни степени n из 1 и только они, называется n-тым *круговым многочленом*. Найдите $\deg \Phi_n$ и покажите, что **а)** $x^n - 1 = \prod_{d|n} \Phi_d(x)$ **б)** $\Phi_n(x) = \prod_{d|n} \left(x^{n/d} - 1\right)^{\mu(d)}$ **в)** $\Phi_{2n}(x) = \Phi_n(-x)$ при нечётном n **г)** $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ при простом $p \nmid n$, $p > 2$ **д)** $\Phi_p(x) = x^{p-1} + \dots + x + 1$ и $\Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right)$ для простых p **е)** $\Phi_{p_1^{k_1} \cdots p_n^{k_n}}(x) = \Phi_{p_1 p_2 \cdots p_n}\left(x^{p_1^{k_1-1} \cdots p_n^{k_n-1}}\right)$ при простых $p_i \neq p_j$ **ж)** $\Phi_n \in \mathbb{Z}[x]$ при всех $n \in \mathbb{N}$.

А3½◇5. Обозначим через i_m число неприводимых приведённых многочленов степени m в $\mathbb{F}_p[x]$. Докажите в $\mathbb{Q}[\![t]\!]$ равенство $(1 - pt)^{-1} = \prod_{m \in \mathbb{N}} (1 - t^m)^{-i_m}$.

А3½◇6. Используя подходящую модификацию обращения Мёбиуса, докажите, что число неприводимых многочленов степени n в $\mathbb{F}_p[x]$ равно $\frac{1}{n} \sum_{d|n} p^d \mu(n/d)$.

А3½◇7. Покажите, что в конечном поле $\mathbb{F}_q$ из q элементов порядок любого элемента мультипликативной группы $\mathbb{F}_q^*$ делит $q-1$. Пользуясь обращением Мёбиуса, найдите для каждого $d|(q-1)$ число элементов d-того порядка в $\mathbb{F}_q^*$. Сколько в $\mathbb{F}_q^*$ элементов порядка $(q-1)$? Какова степень минимального многочлена[1] такого элемента над простым подполем $\mathbb{F}_p \subset \mathbb{F}_q$?

Алгебра инцидентности локально конечного чума. ЧУМ называется *локально конечным*, если $\forall\, x, y$ *отрезок* $[x, y] \stackrel{\text{def}}{=} \{\, z \mid x \leqslant z \leqslant y \,\}$ конечен. Для такого ЧУМа $\mathfrak{P}$ обозначим через $\mathcal{A}(\mathfrak{P})$ множество функций $\varrho : \mathfrak{P} \times \mathfrak{P} \to \mathbb{C}$, которые зануляются на всех (x, y), не находящихся в отношении $x \leqslant y$, и зададим в $\mathcal{A}(\mathfrak{P})$ сложение $\varrho_1 + \varrho_2 : (x, y) \mapsto \varrho_1(x, y) + \varrho_2(x, y)$ и умножение $\varrho_1 \star \varrho_2 : (x, y) \mapsto \sum_{x \leqslant z \leqslant y} \varrho_1(x, z)\varrho_2(z, y)$.

А3½◇8. Покажите, что $\mathcal{A}(\mathfrak{P})$ является (некоммутативным) кольцом с единицей, и $\varrho \in \mathcal{A}(\mathfrak{P})$ обратим если и только если $\forall\, x \in \mathfrak{P}\ \varrho(x, x) \neq 0$.

А3½◇9. Убедитесь, что функция $\zeta(x, y) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ при } x \leqslant y \\ 0 \text{ иначе} \end{cases}$ обратима в $\mathcal{A}(\mathfrak{P})$ и обратная функция $\mu \stackrel{\text{def}}{=} \zeta^{-1}$ удовлетворяет равенствам[2] $\mu(x, y) = -\sum_{x \leqslant z < y} \mu(x, z) = -\sum_{x < z \leqslant y} \mu(z, y)$.

А3½◇10 (обращение Мёбиуса в чуме). Пусть $\mathfrak{P}$ — локально конечный ЧУМ с нижней гранью[3]. Покажите, что любая функция $g : \mathfrak{P} \to \mathbb{C}$ восстанавливается по значениям своих сумм $\sigma(x) = \sum_{y \leqslant x} g(y)$ по формуле $g(x) = \sum_{y \leqslant x} \sigma(y)\mu(y, x)$.

А3½◇11. Найдите функции Мёбиуса для **а)** ЧУМа $\mathbb{N}$ с отношением $n|m$ **б)** ЧУМа $\mathfrak{F}(M)$ всех конечных подмножеств[4] произвольного множества M с отношением $X \subseteq Y$. Во что превращается в этих случаях предыдущая формула обращения?

---

[1]Т. е. приведённого многочлена наименьшей степени, для которого он является корнем.
[2]Запись $x < y$ означает, что $x \leqslant y$ и $x \neq y$.
[3]Т. е. таким $m \in \mathfrak{P}$, что $m \leqslant x\ \forall\, x \in \mathfrak{P}$.
[4]Включая пустое подмножество.