Обращение Мёбиуса

А2½◇1 (функция Мёбиуса). Функция Мёбиуса $\mu : \mathbb{N} \to \mathbb{N} \cup \{0\}$ переводит $n > 1$ в 0, если n делится на квадрат простого числа, и в $(-1)^s$, где s — число простых делителей числа n, если n не делится на квадраты простых чисел, а $\mu(1) \overset{\text{def}}{=} 1$. Докажите, что

а) $\mu(mn) = \mu(m)\mu(n)$ если НОД$(m, n) = 1$

б) $\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ при } n = 1 \\ 0 \text{ при } n > 1. \end{cases}$

А2½◇2 (обращение Мёбиуса). Пусть для функции $g : \mathbb{N} \to \mathbb{C}$ при каждом $n \in \mathbb{N}$ известно значение суммы $\sigma_g(n) = \sum_{d|n} g(d)$. Покажите, что $g(n) = \sum_{d|n} \sigma_g(d) \cdot \mu(n/d)$.

А2½◇3. Для натурального $m > 1$ вычислите $\sum_{d|m} \varphi(d)$, где φ — функция Эйлера.

А2½◇4 (круговые многочлены). Многочлен $\Phi_n(x) = \prod_{\zeta \in R_n} (x - \zeta) \in \mathbb{C}[x]$, где произведение берётся по множеству $R_n \subset \mathbb{C}$ всех комплексных первообразных корней степени n из единицы, называется *n-тым круговым многочленом*. Найдите $\deg \Phi_n$ и докажите, что

а) $x^n - 1 = \prod_{d|n} \Phi_d(x)$

б) $\Phi_n(x) = \prod_{d|n} \left(x^{n/d} - 1\right)^{\mu(d)}$ (модифицируйте обращение Мёбиуса)

в) $\Phi_{2n}(x) = \Phi_n(-x)$ при нечётном n

г) $\Phi_{pn}(x) = \Phi_n\left(x^p\right)/\Phi_n(x)$ при простом $p \nmid n$, $p > 2$

д) $\Phi_p(x) = x^{p-1} + \ldots + x + 1$ и $\Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right)$ для простых p

е) $\Phi_{p_1^{k_1} \ldots p_n^{k_n}}(x) = \Phi_{p_1 p_2 \cdots p_n}\left(x^{p_1^{k_1-1} \cdots p_n^{k_n-1}}\right)$ при простых $p_i \neq p_j$

ж) $\Phi_n \in \mathbb{Z}[x]$ при всех $n \in \mathbb{N}$.

А2½◇5. Обозначим через ι_m число неприводимых приведённых многочленов степени m в $\mathbb{F}_p[x]$. Докажите в $\mathbb{Q}[\![t]\!]$ равенство $(1 - pt)^{-1} = \prod_{m \in \mathbb{N}} \left(1 - t^m\right)^{-\iota_m}$.

А2½◇6. Используя подходящую модификацию обращения Мёбиуса, докажите, что число неприводимых многочленов степени n в $\mathbb{F}_p[x]$ равно $\frac{1}{n} \sum_{d|n} p^d \mu(n/d)$.

А2½◇7. Пусть $\mathbb{F}_q$ — конечное поле из q элементов.

а) Покажите, что порядок любого элемента $\zeta \in \mathbb{F}_q^\times$ делит $q - 1$.

б) При помощи надлежащего обращения Мёбиуса для каждого $d|(q - 1)$ найдите число элементов порядка d в $\mathbb{F}_q^\times$. Сколько в $\mathbb{F}_q^\times$ элементов порядка $q - 1$?

в) Какова степень минимального многочлена элемента $(q - 1)$-го порядка над простым подполем $\mathbb{F}_p \subset \mathbb{F}_q$?

г) Выведите из предыдущего, что любые два поля из q элементов изоморфны.

Персональный табель ______________________________________ . **Листок № 2$\frac{1}{2}$ (необязательный)**

(напишите свои имя, отчество и фамилию)

№	дата	кто принял	подпись
1а			
б			
2			
3			
4а			
б			
в			
г			
д			
е			
ж			
5			
6			
7а			
б			
в			
г			