Конечные поля

A2.1. Обозначим через Fr_n многочлен $x^{p^n} - x$ над полем $\mathbb{F}_p$. Докажите, что:

а) Если f — неприводимый многочлен степени d и $d|n$, то $f|Fr_n$.

б) Многочлен Fr_n является произведением всех неприводимых многочленов степеней, делящих n.

в) Если I_d — количество неприводимых многочленов степени d в $\mathbb{F}_p[x]$, то

$$\sum_{d|n} d \cdot I_d = p^n.$$

A2.2. Для двух последовательностей (a_k) и (b_l) определим их *свертку* формулой

$$(a * b)_n = \sum_{kl=n} a_k b_l.$$

а) Докажите, что свертка задает на последовательностях структуру ассоциативной алгебры с единицей (δ_n).

б) Докажите, что *функция Мёбиуса* μ_n, равная $(-1)^k$ при $n = p_1 p_2 \dots p_k$ и 0 для чисел не свободных от квадратов, является обратной к последовательности из одних единиц ("формула обращения Мёбиуса").

A2.3. Найдите количество I_n неприводимых многочленов степени n над полем $\mathbb{F}_p$ и докажите, что оно больше нуля при любом n (отсюда следует, в частности, что при любом n существует поле из p^n элементов).

Циклотомические поля

A2.4. Обозначим через Φ_n "n-й круговой многочлен", т. е. многочлен $\prod(x - \zeta_n)$, где произведение берется по всем примитивным корням степени n из единицы. Докажите следующие утверждения:

а) $\Phi_p(x) = \frac{x^p - 1}{x - 1}$;

б) $\prod_{d|n} \Phi_d(x) = x^n - 1$.

в) Круговой многочлен — многочлен с целыми коэффициентами и старшим коэффициентом 1.

г*) $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$.

A2.5. Докажите, что многочлен Φ_n неприводим над $\mathbb{Z}$.

Указание. Докажите, что если ζ — корень одного из неприводимых сомножителей Φ_n, то ζ^p — корень *того же* сомножителя (где p — произвольное простое число, не делящее n).

A2.6. а) Пусть p — нечетное простое число, не делящее n, Φ_n — n-й круговой многочлен, рассматриваемый как многочлен над $\mathbb{F}_p$. Докажите, что тогда корни многочлена Φ_n суть элементы порядка n в $\mathbb{F}_p^\times$.

б) Докажите, что, что если p — простой делитель целого числа $\Phi_n(a)$, не делящий n, то $p \equiv 1 \pmod{n}$.

в) Докажите, что для любого целого n существует бесконечно много простых чисел, сравнимых с единицей по модулю n (напомним, что *теорема Дирихле* утверждает, что единицу можно заменить на любой обратимый остаток, и это утверждение останется верным).