Избранные главы дискретной математики. Весна 2025г

Задачи с 6 занятия.

Решения этих задач предполагается обсудить на следующем занятии.

(1) Мы выяснили, что число неприводимых многочленов из $\mathbb{F}_p[t]$ степени n, корни которых в $\mathbb{F}_{p^n}$ являются образующими мультиплакативной группы $\mathbb{F}_{p^n}^*$, равно[1]

$$\frac{\varphi(p^n-1)}{n},$$

из чего, в частности, следует, что $\varphi(p^n-1)$ всегда делится на n. Попробуйте найти прямое доказательство этого утверждения, без использования теории конечных полей.

(2) Может ли возвратный[2] многочлен быть минимальным многочленом образующей мультипликативной группы конечного поля? Один такой пример мы знаем: $t^2+t+1 \in \mathbb{F}_2[t]$ для $\mathbb{F}_4$. Есть ли еще?

(3) Покажите, что если неприводимый многочлен $t^n + a_1 t^{n-1} + \ldots + a_n \in \mathbb{F}_p[t]$ является минимальным многочленом образующей мультипликативной группы поля $\mathbb{F}_{p^n}^*$ то его свободный член a_n является образующей мультипликативной группы поля $\mathbb{F}_p^*$.

[1] Напомним, что φ это функция Эйлера, $\varphi(k)$ это количество натуральных чисел, меньших k и взаимно простых с k.

[2] Напомним, что многочлен $a_0 t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_0$ называется возвратным, если $a_k = a_{n-k}\ \forall\ k$.