Задачи по алгебре. II курс, осень 1999 года.
Листок № 4.

1) Пусть p — простое число. Найти в поле $\mathbb{F}_p$ все решения уравнения $y^2 = x^p - x + 1$.
2) Доказать, что число примитивных корней из 1 степени n в произвольном поле $\mathbb{F}$ либо равно нулю, либо равно $\varphi(n)$, где $\varphi(n)$ — функция Эйлера: количество натуральных чисел m таких, что $m \leqslant n$ и $(m,n) = 1$.
3) а) Для каких натуральных k и n число $p^n - 1$ делится на $p^k - 1$ (число p — простое)?
   б) Для каких q_1 и q_2 существует нетривиальный гомоморфизм $\mathbb{F}_{q_1} \to \mathbb{F}_{q_2}$?
4) Какова максимальная степень неприводимого многочлена над $\mathbb{F}_p$, делящего $x^{p^k} - x$?
5) Сколько неприводимых многочленов степеней 2 и 3 над полем $\mathbb{F}_q$?
6) Доказать, что группа автоморфизмов конечного поля $\mathbb{F}_q$ порождена автоморфизмом Фробениуса $a \mapsto a^p$, где p — простое число и $q = p^k$. Каков порядок этой группы?
7) Доказать, что любой неприводимый многочлен $f(x) \in \mathbb{F}_p[x]$, имеющий корень в $\mathbb{F}_{p^k}$, разлагается в $\mathbb{F}_{p^k}[x]$ на линейные множители.
8) Пусть $\mathbb{F}_q$ — конечное поле из q элементов, $f(x) \in \mathbb{F}_q[x]$ — неприводимый многочлен степени k. Доказать, что $f(x)$ делит многочлен $x^{q^n} - x$ тогда и только тогда, когда k делит n.
9) Пусть (a_n) — произвольная числовая последовательность. Положим $b_n = \sum\limits_{d|n} a_d$ для всех натуральных n. Доказать следующую *формулу обращения Мёбиуса*: $a_n = \sum\limits_{d|n} \mu\left(\frac{n}{d}\right) b_d$, где μ — функция Мёбиуса:
$$\mu(n) = \begin{cases} 0, & \text{если } n \text{ делится на квадрат простого числа,} \\ (-1)^k, & \text{если } n \text{ — произведение } k \text{ разных простых чисел,} \\ 1, & \text{если } n = 1. \end{cases}$$
10) Обозначим через $\psi_q(n)$ число неприводимых многочленов степени n со старшим коэффициентом 1 над полем $\mathbb{F}_q$. Доказать равенство
$$n\psi_q(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$