Задачи марта.

Это задачи, связанные с конечными полями. В отличие от прошлых списков эти задачи (за исключением последней) не формулировались на лекции.

Кроме того, на семинаре можно обсудить решение задачи 3 из индивидуального домашнего задания.

(1) Пусть p — простое число, а n натуральное число. Докажите, что $n \mid \varphi(p^n - 1)$, где φ — функция Эйлера.
(2) Докажите, что при $a \neq 0$ многочлен $x^p - x - a$ неприводим над $\mathbb{F}_p$.
(3) $\alpha \in \mathbb{F}_{p^n}$ является образующей мультипликативной группы $\mathbb{F}_{p^n}^*$. Докажите, что минимальный многочлен элемента α не может быть возвратным.
(4) Каким может быть максимальный период последовательности, заданной возвратным многочленом степени n над полем $\mathbb{F}_p$?
(5) Найдите минимальный и характеристический многочлены автоморфизма Фробениуса $\Phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ (напомним, что $\Phi(z) = z^p$), рассматриваемого как линейный оператор на n-мерном линейном пространстве над $\mathbb{F}_p$.
(6) Верно ли, что любое инвариантное подпространство автоморфизма Фробениуса в конечном поле является подполем?
(7) Верно ли, что для любого натурального числа N можно найти такие p и n, что в мультипликативной группе поля $\mathbb{F}_{p^n}$ есть элемент порядка N? Как искать такие p и n в случае, когда они существуют?
(8) В каких случаях мультипликативная группа $(\mathbb{F}_p[x]/(Q(x)^k))^*$ является циклической? ($Q(x)$ — неприводимый многочлен, $k > 1$)? Интересны любые частичные результаты, даже для $Q(x) = x$.
(9) Разложить на множители как многочлен над полем характеристики p (например, конечным полем) определитель

$$\det \begin{pmatrix} x_0 & x_0^p & x_0^{p^2} & x_0^{p^3} & \dots & x_0^{p^n} \\ x_1 & x_1^p & x_1^{p^2} & x_1^{p^3} & \dots & x_1^{p^n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^p & x_n^{p^2} & x_n^{p^3} & \dots & x_n^{p^n} \end{pmatrix}.$$

Пусть $q = p^k$. Разложить на множители как многочлен над полем $\mathbb{F} \supset \mathbb{F}_q$ определитель

$$\det \begin{pmatrix} x_0 & x_0^q & x_0^{q^2} & x_0^{q^3} & \dots & x_0^{q^n} \\ x_1 & x_1^q & x_1^{q^2} & x_1^{q^3} & \dots & x_1^{q^n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^q & x_n^{q^2} & x_n^{q^3} & \dots & x_n^{q^n} \end{pmatrix}.$$

(10) Пусть p и q разные простые числа. Найти количество неприводимых многочленов степени q над $\mathbb{F}_p$.

(11) Докажите, что число неприводимых многочленов степени n над полем $\mathbb{F}_p$ равно

$$\frac{1}{n} \sum_{k|n} \mu(k) p^{\frac{n}{k}},$$

где μ — функция Мебиуса.

(12) Показать, что если α не квадрат в поле $\mathbb{F}$, то α не квадрат ни в каком расширении поля $\mathbb{F}$ нечетной степени и квадрат в каждом расширении четной степени.

(13) Пусть $\beta \in \mathbb{F}_{q^2}$. Показать, что $\beta^{q+1} \in \mathbb{F}_q$. Показать, что для любого элемента $\alpha \in \mathbb{F}_q$ найдется $\beta \in \mathbb{F}_{q^2}$, такой что $\alpha = \beta^{q+1}$.

(14) Пусть $\alpha \in \mathbb{F}_q$ имеет порядок $q-1$. Показать, что тогда найдется $\beta \in \mathbb{F}_{q^2}$ порядка q^2-1, такой что $\alpha = \beta^{q+1}$.

(15) Верно ли, что для любых трех натуральных чисел k, m и n, больших единицы, существует группа и два ее элемента a и b такие, что $\operatorname{ord} a = k$, $\operatorname{ord} b = m$, $\operatorname{ord}(ab) = n$? А если некоторые из значений k, m и n заменить на ∞?