Семинар 2. Ещё о кольцах, полях и абелевых группах

Задача 2.1. Пусть a, m, n – натуральные числа. Найдите НОД
(а) чисел $a^m - 1$ и $a^n - 1$, **(б)** многочленов $x^m - 1$ и $x^n - 1$, **(в)** многочленов $x^{a^m} - x$ и $x^{a^n} - x$.

Задача 2.2. Вычислите остатки от деления многочлена $(x+1)^{2019}$ на многочлены **(а)** $(x-3)$, **(б)** $(x-4)$, **(в)** $(x-3)(x-4)$.

Задача 2.3. Коммутативное кольцо называется факториальным, если любой его элемент однозначно раскладывается на простые (неприводимые) множители. Примерами факториальных колец служат целые числа $\mathbb{Z}$ и кольцо многочленов $\Bbbk[x]$ с коэффициентами в поле. Сформулируйте аккуратно, что значит однозначно и докажите, что евклидово кольцо факториально.

Задача 2.4. Верно ли, что для любого поля $\Bbbk$ имеется бесконечное количество неприводимых многочленов? бесконечное количество неприводимых многочленов сколь угодно большой степени? Что можно сказать про количество простых элементов в произвольном евклидовом кольце.

Задача 2.5. Докажите, что следующие кольца евклидовы и вычислите подходящие функции Эйлера $\varphi_R(a)$, считающие количество обратимых элементов в факторкольце кольца R по главному идеалу, порожденному элементом $a \in R$:
(а) R – кольцо многочленов $\mathbb{F}_p[x]$, норма $N(f(x)) := \deg f(x)$;
(б) R – кольцо гауссовых чисел $\mathbb{Z}[i]$, норма $N(a+bi) := a^2 + b^2$;
(в)* R – числа Эйзенштейна $\mathbb{Z}[\omega]$, где ω – комплексный корень уравнения x^2+x+1, в качестве нормы возьмите $N(a+bw) := a^2 - ab + b^2$.

Задача 2.6. Докажите комбинаторно следующие численные равенства, посчитав разным способом элементы в подходящем (фактор)кольце: **(а)** $\sum_{d|n} \varphi(d) = n$, **(б)** $\sum_{f(x)|g(x)} \varphi_{\mathbb{F}_p[x]}(f(x)) = p^{\deg(g(x))}$.

Задача 2.7.
(а) Рассмотрим башню полей $\Bbbk \subset \mathbb{F}$ и элемент $\alpha \in \mathbb{F}$, удовлетворяющий алгебраическому уравнению $f(\alpha) = 0$. Докажите, что множество значений многочленов $\Bbbk[\alpha]$ образуют промежуточное подполе $\Bbbk \subset \Bbbk[\alpha] \subset \mathbb{F}$; Сколько элементов в $\Bbbk[\alpha]$, если $\Bbbk$ – конечное поле из q элементов;
(б) Докажите, что количество элементов в конечном поле $\mathbb{F}$ характеристики p может быть только p^n.
(в) При каких условиях на числа q, q' конечное поле из q элементов вкладывается в конечное поле из q' элементов.

Задача 2.8. Обозначим за $N_p(d)$ количество приведенных неприводимых многочленов степени d над полем $\mathbb{F}_p$.
(а) Вычислите $N_p(d)$ экспериментально для малых d и $p = 2, 3$. Выпишите неприводимые многочены степени не выше 5 над $\mathbb{F}_2$.
(б) Докажите, что любой неприводимый многочлен $f(x)$ степени $d|n$ делит многочлен $x^{p^n} - x$,
(в) Докажите, что многочлен $x^{p^n} - x$ не имеет кратных корней и любой его неприводимый делитель имеет степень $d|n$,
(г) Докажите равенство $p^n = \sum_{d|n} dN_p(d)$.

Задача 2.9. Функция $\psi : \mathbb{N} \to \mathbb{C}$ называется мультипликативной, если для любых взаимнопростых чисел m, n выполнено $\psi(mn) = \psi(m)\psi(n)$.
(Функция Мёбиуса) Мультипликативная функция Мёбиуса $\mu(n)$ определена на степени простого числа p следующим простым образом $\mu(p^n) = -\delta_{n,1}$. Докажите, что
(а) $\sum_{d|n} \mu(d) = \delta_{n,1}$,
(б) следующие соотношения на (мультипликативные) функции $a, b : \mathbb{N} \to \mathbb{C}$ равносильны:

$$b(n) = \sum_{d|n} a(d) \Leftrightarrow a(n) = \sum_{d|n} \mu(d) b(\frac{n}{d})$$

(в) $\mu(n)$ равна сумме примитивных корней степени n из единицы.
(г) Пользуясь функцией Мёбиуса, найдите формулу для числа $N_p(n)$ неприводимых многочленов степени n над конечным полем $\mathbb{F}_p$.