Конечные поля и конечные тела[1]

Задача 1. Пусть K — конечное поле, $K^\times := K \setminus \{0\}$ — его мультипликативная группа. Тогда в $K^\times$ не более d элементов порядка d.

▷ **Определение 1.** Число обратимых остатков по модулю n называется *функцией Эйлера* числа n и обозначается $\phi(n)$.

Задача 2. а) $\phi(p) = p - 1$; б) $\sum_{d|n} \phi(d) = n$.

Задача 3. Пусть G — коммутативная группа порядка n, $G_d := \{g \in G \mid g^d = 1\}$.
а) Если группа G циклическая, то $|G_d| = d$ при всех d, делящих n.
б) Если $|G_d| \leqslant d$ при всех d, то группа G циклическая.
Указание. Сколько в группе G элементов порядка n?

Задача 4. Мультипликативная группа конечного поля циклическая.

Задача 5. а) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ ("критерий Эйлера").

б) Форма $x^2 + y^2$ представляет 0 по модулю p, если и только если $p \neq 4k + 3$.

Задача 6. Пусть L — конечное поле, K — его q-элементное подполе. Тогда $|L| = q^n$.

▷ Напомним, что *тело* — это кольцо (вообще говоря, некоммутативное), в котором каждый ненулевой элемент обратим ("некоммутативное поле").

Теорема Веддербёрна утверждает, что любое конечное тело является полем.

▷ **Определение 2.** *Центром* кольца R называется множество его элементов, коммутирующих со всеми элементами кольца, $Z(R) = \{a \in R \mid \forall x \in R\ ax = xa\}$.

Централизатором элемента a кольца R называется множество элементов кольца, коммутирующих с этим элементом, $Z_a = \{x \in R \mid ax = xa\}$.

Аналогичным образом определяется центр группы и централизатор элемента группы.

Задача 7. Пусть G — группа. Два ее элемента, g_1 и g_2 называются *сопряженными*, если $\exists h \in H : g_2 = hg_1h^{-1}$.
а) Сопряженность — отношение эквивалентности.
б) Класс сопряженности элемента g имеет размер $|G|/|Z_g|$.

Задача 8. Пусть D — конечное тело, $|Z(D)| = q$.
а) $|D| = q^n$; б) для любого элемента a тела $|Z_a| = q^d$, причем $d \mid n$;
в) $q^n - 1 = q - 1 + \sum \dfrac{q^n - 1}{q^{d_i} - 1}$ (причем все d_i делят n).
Указание. Примените предыдущую задачу к группе $D^\times := D \setminus \{0\}$.

▷ **Определение 3.** n-м *круговым многочленом* называется многочлен $\Phi_n(x) = \prod(x - \zeta_n)$, где произведение берется по всем примитивным корням степени n из единицы.

Задача 9. а) $\Phi_p(x) = x^{p-1} + \ldots + 1$; б) $\deg \Phi_n = \phi(n)$; в) $\prod\limits_{d|n} \Phi_d(x) = x^n - 1$; г) $\Phi_n \in \mathbb{Z}[x]$.

Задача 10. Конечное тело является полем.
Указание. Рассмотрите равенство из задачи 2в) по модулю $\Phi_n(q)$.

Задача 11. а) В кватернионной алгебре над конечным полем $(\mathbb{F}_q[i, j]/(i^2 = j^2 = -1, ij = -ji))$ есть делители нуля.
б) Форма $x^2 + y^2 + z^2 + t^2$ представляет 0 по любому простому модулю.

Задача 12*. Любое целое число является суммой четырех квадратов.

[1] Листок написан по мотивам лекции Д. Каледина 30.03.2013.