Цель этого листка — доказать следующую теорему.

Теорема 1. *В любом конечном поле F найдётся такой элемент x, что все ненулевые элементы F имеют вид x^n, где $n \in \mathbb{N}$.*

Определение 1. Элементы x из теоремы 1 называют *образующими* или *порождающими элементами*.

Положим $p = \mathrm{char} F$, $q = |F|$. Множество ненулевых элементов поля обозначим через F^*.

Как и в полях $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, в любом поле F можно рассмотреть многочлены $F[x]$ над данным полем. Все соответствующие определения (сложение, умножение, деление, степень, корни, остатки, ...) дословно переносятся на $F[x]$. Многие свойства также сохраняются для многочленов над произвольным полем, в частности, свойства из задачи 1а)б).

Задача 1. **а)** Докажите, что элемент a — корень многочлена $f(x) \in F[x]$ если и только если $f(x)$ делится на $x - a$.

б) Докажите, что число различных корней многочлена $f(x) \in F[x]$ не больше $\deg f(x)$.

в) Докажите, что все элементы F^* являются корнями многочлена $x^{q-1} - 1$.

г) Пусть $d \mid (q-1)$. Докажите, что многочлен $x^d - 1$ имеет ровно d различных корней в F^*.

Определение 2. Для элемента $a \in F^*$ обозначим через $d(a)$ *порядок* элемента a, то есть такое минимальное натуральное k, что $a^k = 1$.

Задача 2. Докажите, что

а) $d(a)$ определён и не больше $q - 1$.

б) корни многочлена $x^k - 1$ в F^* — это в точности элементы F^*, у которых порядок делит k.

Задача 3. Найдите порядки элементов из $(\mathbb{Z}/p\mathbb{Z})^*$ при $p = 2, 3, 5, 7$. Какие из этих элементов являются порождающими?

Задача 4. Напомним, что функция Эйлера $\varphi(n)$ определяется, как количество обратимых остатков в $\mathbb{Z}/n\mathbb{Z}$. Докажите тождество:

$$\sum_{d|n} \varphi(d) = n.$$

Указание. Приведите дроби $\frac{1}{n}, \ldots, \frac{n}{n}$ к несократимому виду. Сколько дробей будут иметь знаменатель d (где $d \mid n$)?

Задача 5. Обозначим через $\psi(d)$ количество элементов F^* порядка d. Докажите, что

а) При $k \mid (q-1)$ выполнено $\sum\limits_{d|k} \psi(d) = k$;

б) При $k \mid (q-1)$ выполнено $\psi(k) = \varphi(k)$.

в) Количество элементов порядка $q - 1$ в F^* равно $\varphi(q-1) \geqslant 1$. Выведите отсюда теорему 1.

Задача 6. Проверьте, что указанное множество вычетов образует поле и найдите там порождающий элемент: **а)** $\mathbb{F}_2[x]/(x^2 + x + 1)\mathbb{F}_2[x]$; **б)** $\mathbb{F}_2[x]/(x^3 + x + 1)\mathbb{F}_2[x]$; **в)** $\mathbb{F}_3[x]/(x^2 + x - 1)\mathbb{F}_3[x]$.

Задача 7. Мы найдём сумму $\sum\limits_{x \in F^*} x^k$ разными способами. Пусть $a \in F^*$ — порождающий элемент F.

а) Найдите сумму, используя тот факт, что умножение на a является взаимно-однозначным соответствием F^* на себя.

б) Найдите сумму, используя тот факт, что все элементы F^* являются разными степенями элемента a.

в) Как найти сумму, не используя Теорему 1?

Теорему 1 можно попробовать обобщить с конечных полей на более общие структуры. К примеру, для каждого целого m можно взять вычеты $\mathbb{Z}/m\mathbb{Z}$ по модулю m и найти порождающий элемент в $(\mathbb{Z}/m\mathbb{Z})^*$ (определение порождающего элемента дайте самостоятельно). Он также называется *первообразным корнем по модулю m*.

Задача 8. **а)** Существует ли в $\mathbb{Z}/m\mathbb{Z}$ первообразный корень для $m = 2, 3, 4, 5, 6, 7$?

б) Существует ли такое m, что не существует первообразных корней в $\mathbb{Z}/m\mathbb{Z}$?

Задача 9. Пусть $\varphi(m) = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ — каноническое разложение числа $\varphi(m)$ на простые сомножители, $(g, m) = 1$. В этом случае g — первообразный корень в $\mathbb{Z}/m\mathbb{Z}$ тогда и только тогда, когда g не является решением ни одного из сравнений $g^{\frac{\varphi(m)}{p_k}} \equiv 1 \pmod m$ при $k = 1, \ldots, s$.

Задача 10. Найдите какой-нибудь первообразный корень по модулю **а)** 11; **б)** 17.

Задача 11. Докажите критерий Вильсона (листок 23, задача 12), используя существование первообразных корней по простому модулю.

1 а	1 б	1 в	1 г	2 а	2 б	3	4	5 а	5 б	5 в	6 а	6 б	6 в	7 а	7 б	7 в	8 а	8 б	9	10 а	10 б	11