

---

**Практика №1**

---

**2. Мультипликативная группа конечного поля.**

1. Найти все примитивные корни поля  $\mathbb{F}_{31}$ .
2. Найти порядки всех элементов группы  $\mathbb{F}_{17}^*$ .
3. Сколько примитивных корней существует в поле  $\mathbb{F}_{257}$ ?
4. Доказать, что если  $m$  и  $n$  взаимно просты, то

$$(\mathbb{Z}/mn)^* \cong (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*.$$

5. Представить группу  $(\mathbb{Z}/36)^*$  как произведение циклических групп. Найти порядки этих групп.

**3. Многочлены над конечными полями.**

1. Как много многочленов степени 4 существует над полем  $\mathbb{F}_4$ ?
2. Как много многочленов степени 3 существует над полем  $\mathbb{F}_3, \mathbb{F}_4$ ?
3. Для многочленов  $f(x) = x^4 + 1$  и  $g(x) = x^2 + x + 1$  над  $\mathbb{F}_2$ 
  - найти многочлены  $u(x), v(x) \in \mathbb{F}_2[x]$ , такие, что

$$u(x)f(x) + v(x)g(x) = 1.$$

- вычислить  $g^{10}(x) \bmod f(x)$ .