# 1 Конечные поля

**Определение 1.1** (Конечное поле)**.**

**Следствие 1.2.** *Конечные поля имеют конечную характеристику*

Доказательство.

$$\underbrace{1+...+1}_{n} = \underbrace{1+...+1}_{m} \qquad n = m$$

$$\underbrace{1+...+1}_{n} = 0$$

Что это вообще такое □

**Теорема 1.3.** *Если $F$ - конечное поле характеристики $p$, то $|F| = p^k$*

Доказательство. Так как $F$ - конечное поле $\mathbb{Z}_p \subseteq F$, тогда $F$ - линейное пространство (почему это линейное пространство) над $\mathbb{Z}_p$, в таком случае имеется базис $e_1, ..., e_k$. Пусть $a \in F$б тогда

$$a = a_1e_1 + ... + a_ke_k \quad a_1, ..., a_k \in \mathbb{Z}_p$$

И так как $|\mathbb{Z}_p| = p$, то $|F| = p^k$ - количество комбинаций $a_1, ..., a_k$ □

**Следствие 1.4.** *Если $m \neq p$, то поля из $m$ элементов не существует*

Доказательство. ??? □

**Теорема 1.5** (Мечта школьника)**.** *Если $F$ - поле характеристики $p$, то*

$$(x+y)^p = x^p + y^p$$

Доказательство. Пусть $x, y \in F$, тогда по формуле бинома ньютона

$$(x+y)^p = \sum_{i=0}^{p} C_p^i x^i y^{p-i}$$

Рассмотрим первый и последний элемент этой суммы. По формуле сочетания

$$C_p^0 = \frac{p!}{0!(p-0)!} = 1$$

$$C_p^p = \frac{p!}{p!(p-p)!} = 1$$

поэтому

$$\begin{aligned}(x+y)^p &= \sum_{i=0}^{p} C_p^i x^i y^{p-i} \\ &= C_p^0 x^0 y^p + \sum_{i=1}^{p-1} C_p^i x^i y^{p-i} + C_p^p x^p y^0 \\ &= y^p + \sum_{i=1}^{p-1} C_p^i x^i y^{p-i} + x^p\end{aligned}$$

Рассмотрим оставшуюся часть суммы, то есть для $i \neq 0 \neq p$. По формуле сочетания

$$C_p^i = \frac{p!}{i!(p-i)!} = p \cdot c_i \quad i \neq 0 \neq p$$

где $c_i$ - некоторое число, зависимое от $i$. Подставляя $C_p^i$ получаем

$$\sum_{i=1}^{p-1} C_p^i x^i y^{p-i} = \sum_{i=1}^{p-1} p c_i x^i y^{p-i} = \sum_{i=1}^{p-1} \underbrace{(1+...+1)}_{p} c_i x^i y^{p-i} = 0$$

так как элемент $p \in F$ равен нулю. Таким образом

$$(x+y)^p = y^p + \sum_{i=1}^{p-1} C_p^i x^i y^{p-i} + x^p = x^p + y^p$$

□

**Теорема 1.6.** *Если $F$ - поле характеристики $p$, то*

$$((x+y)^p)^k = (x^p)^k + (y^p)^k$$

Доказательство.

$$\begin{aligned}(x+y)^{p^k} &= ((x+y)^p)^{p^{k-1}} \\ &= (x^p + y^p)^{p^{k-1}} \\ &= ((x^p + y^p)^p)^{p^{k-2}} \\ &= ... \\ &= (x^{p^{k-1}} + y^{p^{k-1}})^{p^1} \\ &= x^{p^k} + y^{p^k}\end{aligned}$$

□

**Теорема 1.7.** *Если $F$ - конечное поле и $|F| = m$, тогда существует корень уравнения типа $x^{m-1} - x$*

Доказательство. Пусть $F' = \{F \setminus \{0\}, \cdot, 1, -1\}$, $F'$ является группой и $|F'| = m - 1$. Пусть $a \in F'$, тогда по **??**

$$a^{m-1} = 1$$

То есть все ненулевые элементы группы удовлетворяют $x^{m-1} = 0$.

Так как $x^m - x = x(x^{m-1} - 1)$, то и нулевой элемент и ненулевые элементы являются корнями этого уравнения. □

**Теорема 1.8.** *Если существует поле $F$, такое что $|F| = p^k$, то существует поле $F'$, такое что $|F'| = p^{k'}$, при любом $k' \leq k$*

Доказательство. Если $a|b$, то $(x^a - 1)|(x^b - 1)$ (как так). Предположим $b = ac$, то есть

$$x^b = (x^a)^c - 1 = (x^a - 1)((x^a)^{c-1} + (x^a)^{c-2} + ... + x^a + 1)$$

$F$ - корни многочлена $x^{p^k} - x = x(x^{p^{k-1}} - 1)$

Что дальше в этой теореме? □

Что дальше в этой главе?