# *Теорема о нулях.*

***Теорема 1.*** *Пусть $\mathbb{F}$ – поле и $f \in \mathbb{F}[x_1, \ldots, x_n]$ - ненулевой многочлен суммарной степени $\sum_{i=1}^{n} m_i$, в котором коэффициент при $x_1^{m_1} \ldots x_n^{m_n}$ отличен от 0. Тогда для произвольных множеств $S_1, \ldots, S_n \subseteq \mathbb{F}$ с $|S_i| > m_i, 1 \leq i \leq n$, существуют $c_i \in S_i$ такие, что $f(c_1, \ldots, c_n) \neq 0$.*

*Для доказательства теоремы мы используем две леммы:*

*Л е м м а 1. Предположим, что $f$ как многочлен от $x_i$ имеет степень $t_i, 1 \leq i \leq n$, и пусть $S_i \subseteq \mathbb{F}, |S_i| > t_i$. Тогда если $f(x_1, \ldots, x_n) = 0$ для всякого набора $(x_1, \ldots, x_n) \in S_1 \times \ldots \times S_n$, то $f \equiv 0$.*

*Л е м м а 2. Пусть$g_i = \prod_{s \in S_i}(x_i - s)$,$1 \leq i \leq n$, - многочлен от переменной $x_i$. Если многочлен $f$ равен нулю в каждой точке, принадлежащей $S_1 \times \ldots \times S_n$, то существуют такие многочлены $h_1, \ldots h_n \in \mathbb{F}[x_1, \ldots, x_n]$, что*

$$f = \sum_{1 \leq i \leq n} h_i \, g_i$$

*и при этом $deg h_i \leq deg\, f - deg g_i$ при всех i.*

*Упражнения*

1. *Докажите теорему Коши-Дэвенпорта:*

*Пусть p – простое число, $A$ и $B$ – множества остатков при делении на p. Определим $A + B$ как множество всех остатков по модулю p от сумм вида $a + b$, где $a \in A$, $b \in B$. Докажите, что*

$$|A + B| \geq min\{p, |A| + |B| - 1\}.$$

2. *Пусть $d, n \in N$ и p – простое число. Тогда существуют такие $x_1, \ldots, x_d \in Z$, что $x_1^d + \cdots + x_d^d \equiv n \ (mod\ p)$.*

***Теорема 2***. *Пусть p – простое число и пусть* $f_1, \dots, f_k \in \mathbb{F}_p[x_1, \dots, x_n]$ − *многочлены над* $\mathbb{F}_p$ *от n переменных, такие что* $f_i(0, \dots, 0) = 0$ *для* $1 \le i \le k$ *Пусть* $S_1, \dots, S_n \subseteq \mathbb{F}_p$ − *подмножества* $\mathbb{F}_p$, *такие что* $0 \in S_j$ *для всякого j и*

$$\sum_{j=1}^{n}(|S_j| - 1) > (p-1)(\, deg f_1 + \dots + deg f_k).$$

*Тогда система*

$$f_i(x_1, \dots, x_n) = 0, \ 1 \le i \le k,$$

*имеет решение* $(x_1, \dots, x_n) \in S_1 \times \dots \times S_k$, *отличное от* $(0, \dots, 0)$.

*Упражнение 3. Дано натуральное число* $k$ *и простое число p. Пусть также* $S_1, \dots, S_n \subseteq \{0,1,2, \dots, p-1\}$ − *множества, содержащие 0 и такие, что* $\sum_{i=1}^{n}(|S_i| - 1) \ge 1 + k(p-1)$. *Пусть* $a_{ij}$, $1 \le j \le k, 1 \le i \le n$ − *произвольные целые числа. Тогда существуют элементы* $x_i \in S_i, 1 \le i \le n$, *не все равные 0, такие что*

$$a_{j1}x_1 + a_{j2}x_2 + \dots + a_{jn}x_n \equiv 0 \ \ (mod\, p)$$

*Для всех j* $\in \{1,2, \dots, k\}$.

*Упражнение 4. Пусть p – простое число и G – неориентированный граф, у которого средняя степень вершин больше 2p-2, а максимальная степень вершины - не больше 2p-1. Тогда из G можно удалить несколько вершин и рёбер так, что степень каждой оставшейся вершины будет равна p.*

***Теорема** 3 ( гипотеза Эрдеша-Гайлбронна).*

*Рассмотрим простое число p и множества* $A, B \subseteq \mathbb{F}_p$ *.Определим* $A \dot{+} B$ *как множество всех остатков по модулю p от сумм вида* $a + b$ *где* $a \in A$, $b \in B$, $a \ne b$. *Докажите, что*

$$|A \dot{+} A| \ge min\{p, 2|A| - 3\}.$$

*Для самостоятельного решения:*

*1. Пусть p – простое число и G – граф, в котором не меньше 2p-1 вершин. Докажите, что существует непустое множество U вершин G, такое что количество ребер G, имеющих хотя бы одну вершину в U, делится на p.*

*2.Дано натуральное число n. Рассмотрим множество :*

$$S = \{\ (x, y, z)\ | x, y, z \in \{0,1, \dots, n\}, x + y + z > 0\ \},$$

*состоящее из* $(n+1)^3 - 1$ *точек трёхмерного пространства. Найдите наименьшее возможное количество плоскостей, объединение которых содержит все точки множества S, но не содержит точку* $(0,0,0)$.

*3. (Теорема Эрдеша-Гинзбурга-Зива). Докажите, что для любого натурального* $n$ *из произвольного набора из* $2n-1$ *натуральных чисел можно выбрать* $n$ *чисел, сумма которых кратна* $n$.

*4*. Рассмотрим множества* $A = \{a_1, \dots, a_k\} \subseteq \mathbb{F}_p$ *и* $B = \{b_1, \dots, b_k\} \subseteq \mathbb{F}_p$, *где p – нечётное простое число. Докажите, что существует перестановка* $(s_1, \dots, s_k)$ *множества* $(1, 2, \dots, k)$, *такая что элементы* $a_i + b_{s_i} \in \mathbb{F}_p, 1 \leq i \leq k$ *попарно различны.*