## Избранные главы дискретной математики.

### Задачи с занятия 4.

1) Пусть $p$ – простое число, $W_n = \mathbb{F}_p^{\mathbb{F}_p^n}$ — множество функций от $n$ переменных, т.е. функций $f : \mathbb{F}_p^n \to \mathbb{F}_p$. Тогда $W_n$ это $p^n$-мерное линейное пространство над полем $\mathbb{F}_p$. Рассмотрим линейное отображение $\sigma : W_n \to W_n$, сопоставляющее каждой функции $f \in W_n$ новую функцию $\sigma(f) : \mathbb{F}_p^n \to \mathbb{F}_p$, задаваемую формулой

$$\sigma(f)(x_1, \ldots, x_n) = \sum_{\substack{0 \le k_1 \le p-1 \\ \cdots \\ 0 \le k_n \le p-1}} f(k_1, \ldots, k_n) x_1^{k_1} \ldots x_n^{k_n}.$$

а) Докажите, что при $p = 2$ $\sigma$ является инволюцией (т.е. $\sigma^2 = \mathrm{Id}$).
б) Как(при $p = 2$) описать инвариантные функции, т.е. такие, что $\sigma(f) = f$? Сколько их?
в) Как(при $p = 2$) описать образ оператора $\sigma + \mathrm{Id}$?
г) Что можно сказать об отображении $\sigma$ при $p > 2$? (Я не знаю даже намека на ответ...)

2) Обосновать следующий способ вычисления многочлена Жегалкина булевой функции $f(x_1, \ldots, x_n)$. В первый столбец матрицы $X$ размером $2^n \times 2^n$ выписываются значения функции $f$ при лексикографическом упорядочении переменных. Каждый следующий, $k+1$-ый столбец вычисляется по $k$-ому столбцу по следующей формуле:

$$X_{i,k+1} = X_{i,k} + X_{i+1,k}, \qquad i = 1, \ldots, 2^n - k.$$

(Тем самым мы заполняем только часть матрицы, лежащую не ниже побочной диагонали.) После заполнения всех столбцов коэффициенты многочлена Жегалкина в лексикографическом порядке считываются из первой строки.