Квантовый бином и его родственники

Задача 3.0. а) Пусть q — степень простого числа. Найдите (выразите через $[n]!$) $|GL_n(\mathbb{F}_q)|$, количество обратимых матриц над полем из q элементов.

б) Если q — степень простого числа, то $\begin{bmatrix} n \\ k \end{bmatrix}$ есть $|Gr_{k,n}(\mathbb{F}_q)|$, количество k-мерных линейных подпространств в n-мерном пространстве над полем из q элементов.

в*) Если $q = -1$, то $\begin{bmatrix} n \\ k \end{bmatrix}$ есть $\chi(Gr_{k,n}(\mathbb{R}))$, Эйлерова характеристика вещественного Грассманиана k-мерных плоскостей в n-мерном пространстве.

Задача 3.1. а) $[n]!$ является (как многочлен от q) производящей функцией перестановок n элементов по числу беспорядков.

б) Найдите среднее число беспорядков в перестановке n элементов.

Задача 3.2. На лекции объяснялось, что

$$(1+qx)(1+q^2x)\dots(1+q^nx) = \sum q^{\frac{k(k+1)}{2}} \begin{bmatrix} n \\ k \end{bmatrix} x^k.$$

Докажите другую версию q-бинома: если $YX = qXY$ (а q со всеми переменным коммутирует), то

$$(X+Y)^n = \sum \begin{bmatrix} n \\ k \end{bmatrix} X^{n-k}Y^k.$$

Задача 3.3. Сформулируйте и докажите q-аналог тождества Вандермонда $\binom{m+n}{k} = \sum_{i+j=k} \binom{m}{i}\binom{n}{j}$.

Задача 3.4. Хорошо известно, что $\sum_k (-1)^k \binom{n}{k} = 0$. Найдите сумму $\sum_k (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}$.

Задача 3.5*. а) Пусть $\zeta^p = 1$. Найдите при помощи предыдущего тождества (для $n = p-1$ и $q = \zeta$) сумму $\sum \zeta^{-k(k-1)/2}$ и докажите, что

$$g(p) := \sum \zeta^{k^2} = \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}).$$

б) Выведите отсюда, что $g(p)^2 = (-1)^{\frac{p-1}{2}} p$. Если знаете, как отсюда следует квадратичный закон взаимности — порадуйтесь[1].

Задача 3.6. а) Вспомните лекцию и докажите, что $\displaystyle\prod \frac{1-q^n}{1+q^n} = 1 + 2\sum_{k\geq 1} (-1)^k q^{k^2}$.

б*) Придумайте комбинаторное доказательство.

Задача 3.7. Сколько существует нильпотентных матриц порядка n над полем из q элементов? q-деформацией какой задачи это естественно считать?

[1] Если не знаете, то можно начать со следующего. Пусть $p = 4k+1$, $l \equiv 1 \pmod{p}$ простое. Тогда в $\mathbb{Z}/l$ есть корень степени p из единицы — а значит, по доказанному выше, в $\mathbb{Z}/l$ есть квадратный корень из p (а именно, $g(p)$). На самом деле, при $p = 4k+1$ условие $l \equiv 1 \pmod{p}$ можно ослабить до $l \equiv a^2 \pmod{p}$, т. е. «p квадрат по модулю $l \iff l$ квадрат по модулю p».