

54. Матрицы Адамара. (Первая) конструкция Пэли с квадратичными вычетами при $n = p + 1, p = 4m + 3$.

Определение: Для простого p определим $p \times p$ матрицу Якобсталя Q формулой $Q_{jl} = \left(\frac{j-l}{p}\right)$ (это символ Лежандра).

Конструкция Пэли: Пусть $p \equiv 3 \pmod{4}$. Тогда матрица

$$\begin{pmatrix} 1 & e^T \\ e & Q - E_p \end{pmatrix}$$

где e — столбец из единиц, а E_p — единичная матрица, является матрицей Адамара порядка $p + 1$.

▲ Рассмотрим скалярное произведение строк a_1 и a_2 матрицы Q .

$$\sum_{b=1}^p \left(\frac{a_1 - b}{p}\right) \left(\frac{a_2 - b}{p}\right)$$

Пусть $x = a_1 - b, c = a_2 - a_1$. Получаем

$$\sum_{x=1}^p \left(\frac{x}{p}\right) \left(\frac{c+x}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \left(\frac{x \cdot x^{-1}(x+c)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right)^2 \left(\frac{1+x^{-1}c}{p}\right)$$

При $x \neq 0$ $\left(\frac{x}{p}\right)^2 = 1$. Положим $y = 1 + x^{-1}c$. Так как $c \not\equiv 0 \pmod{p}$, то $x^{-1}c$ пробегает все числа $1 \dots p-1 \Rightarrow y$ пробегает числа $2 \dots p$.

$$\sum_{x \not\equiv 0 \pmod{p}} \left(\frac{1+x^{-1}c}{p}\right) = \sum_{y \not\equiv 1 \pmod{p}} \left(\frac{y}{p}\right) = 0 - \left(\frac{1}{p}\right) = -1$$

Рассмотрим скалярное произведение строк искомой матрицы. По сравнению со скалярным произведением строк Q добавятся слагаемые $1, (-1) \cdot \left(\frac{a_1-a_2}{p}\right)$ и $(-1) \cdot \left(\frac{a_2-a_1}{p}\right)$ (раньше они умножались на нули). Эти символы Лежандра отличаются в $\left(\frac{-1}{p}\right)$ раз. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4m+2}{2}} = (-1)^{2m+1} = -1 \Rightarrow$ слагаемые с символом Лежандра сократятся \Rightarrow скалярное произведение любых двух строк искомой матрицы равно $(-1) + 1 = 0$.

Очевидно, что если мы рассмотрим скалярное произведение первой строки с любой другой, мы получим 0, так как в Q было поровну единиц и минус единиц (ранее доказывалось, что в \mathbb{Z}_p поровну квадратичных вычетов и невычетов) и у нас добавилась одна единица и одна минус единица. \Rightarrow это матрица Адамара ■