81 Сумма Гаусса

Для начала узнаем, чему равны следующие суммы:

$$\sum_{k=1}^{k} e^{2\pi ix}$$

Она с очевидностью равна k, т.к. $e^{2\pi ix} = 1 \ \forall x \in N$

Теперь рассмотрим такую сумму:

$$\sum_{x=1}^{q} e^{2\pi i \frac{ax}{q}}, \text{ где } (a,q) = 1$$

$$\sum_{x=1}^{q} e^{2\pi i \frac{ax}{q}} = e^{2\pi i \frac{a}{q}} * (\frac{e^{2\pi i a} - 1}{e^{\frac{2\pi i a}{q} - 1}}) = 0$$

Таким образом, если а и q взаимнопросты, сумма равна 0, иначе - q

 $\mathit{Суммой}\ \mathit{Гаусса}$ называется сумма вида $S = \sum\limits_{x=1}^q e^{2\pi i \frac{ax^2}{q}}.$ Посчитаем, чему равен ее модуль

$$|S|^2 = S * \overline{S} = \sum_{x=1}^q e^{2\pi i \frac{ax^2}{q}} \sum_{y=1}^q e^{-2\pi i \frac{ay^2}{q}}.$$

Заметим, что суть данной суммы - суммирование по окружности через равные промежуточки. Поэтому разницы нет, начнем мы из точки "у"или из какой-то другой, полученной из "у"сдвигом по этой окружности. Результат не изменится. Поэтому давайте заменим по второй сумме "у"на "x + y". Продолжаем равенство:

рой сумме "у"на "х + у". Продолжаем равенство:
$$= \sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}} \sum_{y=1}^{q} e^{-2\pi i \frac{ay^2 + 2axy + ax^2}{q}} = \sum_{x=1}^{q} \sum_{y=1}^{q} e^{-2\pi i \frac{ay^2 + 2axy}{q}} = \sum_{y=1}^{q} \sum_{x=1}^{q} e^{-2\pi i \frac{ay^2 + 2axy}{q}} = \sum_{y=1}^{q} e^{-2\pi i \frac{ay^2 + 2axy}{q}} =$$

Обозначим
$$b = -2ay$$
; $\sum_{x=1}^q e^{-2\pi i \frac{2axy}{q}} = \sum_{x=1}^q e^{2\pi i \frac{bx}{q}} (*)$

Рассмотрим, каким может быть q

- Пусть q нечетное. Тогда 2а не делится на q, а у делится на q только при y = q. \Longrightarrow (*) = 0 $\forall y \neq q$. При y = q \longrightarrow (*) = q; $|S|^2 = e^{-2\pi i a q} * q = q$
- Пусть q четное. Тогда b делится на q \iff $y=q, \frac{q}{2}$ Рассуждая таким же образом, как в первом пункте, получим, что (*) не обнуляется только при двух значениях у. Тогда посчитаем сумму, учитывая это знание (подставляя в необнулившиеся слагаемые соответствующие у) $|S|^2=1*q+e^{-2\pi i \frac{a}{q}*\frac{q^2}{4}}*q=q+q*e^{\frac{-\pi i a}{2}*q}=\begin{cases} 2q & q\equiv 0(4) \\ 0 & q\equiv 2(4) \end{cases}$

1

Таким образом,

$$|S| = \begin{cases} \sqrt{q} & \text{q - нечетное} \\ \sqrt{2q} & q \equiv 0(4) \\ 0 & q \equiv 2(4) \end{cases}$$