Одеський національний університет імені І. І. Мечникова
Факультет математики, фізики та інформаційних технологій
Кафедра комп'ютерної алгебри та дискретної математики

Кваліфікаційна робота

на здобуття ступеня вищої освіти «бакалавр»

«Суми Гауса над кінцевим полем»

«Gauss's sums over a finite field»

Виконав здобувач денної форми навчання
спеціальності 111 Математика
Освітня програма «Математика»

Гончаренко Юрій Максимович

Керівник док. фіз – мат наук, проф., Варбанець П.Д
(науковий ступінь, вчене звання, прізвище та ініціали, підпис)
Рецензент проф. Варбанець С.П.
(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:
Протокол засідання кафедри
№ ___ від _____2023 р.

Завідувач кафедри

_____ _____
(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК №_____
протокол № ____ від _____ 2023 р.

Оцінка_____/___ ___/_____
(за національною шкалою, шкалою ECTS, бали)

Голова ЕК

_____ _____
(підпис) (прізвище, ініціали)

Одеса – 2023

ЗМІСТ

ВСТУП…… 3

Розділ 1. Суми Гауса над кінцевим полем Z_p…….. 4

Розділ 2. Точне значення сум Гауса…….. 11

Розділ 3. Кватернарні суми Гауса…..…… 18

ВИСНОВКИ……... 28

СПИСОК ВИКОРИСТАНИХ ДЖЕЛЕЛ…….. 29

ВСТУП

В теорії чисел тригонометричні та експотенціальні суми, зокрема суми Гауса, являються важливим інструментом для розв'язання різноманітних проблем, пов'язаних з цілими числами, які часто не можуть бути вирішені за допомогою інших методів. Такі суми можуть бути розглянуті в контексті теорії скінченних полів, де вони також виявляються досить корисними – наприклад, при дослідженні питань щодо кількості розв'язків рівнянь над скінченними полями, а також в різних додатках скінченних полів.

Метою даної роботи є дослідження властивостей сум Гауса над скінченними полями.

Об'єкт дослідження – суми Гауса над скінченними полями.

Предмет дослідження – властивості суми Гауса над скінченними полями.

Згідно з метою дослідження було поставлено наступні *завдання*:

- означити суму Гауса над скінченними полями;
- довести основні теореми для суми Гауса при $n \geq 5$;
- сформулювати та довести основні леми теорії сум Гауса;
- дослідити питання точного значення сум Гауса;
- дослідити кватернарні суми Гауса.

Робота складається з трьох розділів, кожен з яких містить представлені доведення основних теорем та лем теорії суми Гауса.

Розділ 1. Суми Гауса над кінцевим полем Z_p

Розглянемо наступну суму- суму Гауса:

$$S(a,D)=\sum_{x=1}^{D-1} e^{2\pi i\cdot\frac{a}{D}\pi^2} \quad (1.1)$$

D – ціле, додатнє $(a,D)=1$. Зрозуміло, що значення суми буде одним і тим же, якщо x пробігає будь-яку повну систему лишків по модулю D.

Лема 1.1. Нехай $(a,D)=1$. *Тоді:*

$$|S(a,D)|=\begin{cases}\sqrt{D}, & D-\text{непарне},\\ \sqrt{2D}, & D-\text{кратне 4},\\ 0, & D\equiv 2(mod\ 4).\end{cases} \quad (1.2)$$

Доведення:

$$|S(a,D)|^2=\sum_{x_1=0}^{D-1} e^{2\pi i\cdot\frac{a}{D}{x_1}^2}\sum_{x_2=0}^{D-1} e^{-2\pi i\cdot\frac{a}{D}{x_2}^2}=\sum_{x_1=0}^{D-1}\sum_{x_2=0}^{D-1} e^{2\pi i\cdot\frac{a}{D}\left({x_1}^2-{x_2}^2\right)}. \quad (1.3)$$

Робимо заміну: $x_1=x_2+t$. Коли x_1 та x_2 пробігають повну систему лишків по модулю D, то x_2 та t пробігають незалежно повні системи лишків по модулю D.

$$|S(a,D)|^2=\sum_{t=0}^{D-1}\sum_{x_2=0}^{D-1} e^{2\pi i\cdot\frac{at^2+2atx_2}{D}}=\sum_{t=0}^{D-1} e^{2\pi i\cdot\frac{at^2}{D}}\sum_{x_2=0}^{D-1} e^{2\pi i\cdot\frac{2at}{D}x_2}. \quad (1.4)$$

а) Нехай D непарне, $(2a,D)=1$

$$\sum_{x_2=0}^{D-1} e^{2\pi i\cdot\frac{2atx_2}{D}}=\begin{cases}D, & D|t,\\ D, & D\nmid t\end{cases} \quad (1.5)$$

Тому

$$|S(a,D)|^2=e^{2\pi i\cdot\frac{a0^2}{D}}\cdot D=D,\qquad |S(a,D)|=\sqrt{D}. \quad (1.6)$$

б) Нехай D парне, $D=2D',\ (a,\ D')=1$

$$|S(a,D)|^2 = \sum_{t=0}^{D-1} e^{2\pi i \cdot \frac{at^2}{D}} \sum_{x_2=0}^{D-1} e^{2\pi i \cdot \frac{2atx_2}{D}} \qquad (1.6)$$

$$\sum_{x_2=0}^{D-1} e^{2\pi i \cdot \frac{2atx_2}{D'}} = \begin{cases} 2D', & \text{при } t = 0, \quad t = D' \\ D, & \text{при інших значеннях } t \end{cases} \qquad (1.7)$$

$$|S(a,D)|^2 = 2D' \cdot \left(e^{2\pi i \cdot \frac{a0^2}{D'}} + e^{2\pi i \cdot \frac{aD'}{2D'}} \right) = 2D' \cdot \left(1 + e^{2\pi i \cdot \frac{aD'^2}{2}} \right) \qquad (1.8)$$

Якщо D' - парне, то $|S(a,D)|^2 = 4D'$, $|S(a,D)|^2 = 2D$, (a – непарне в силу $(a,D) = 1$). Якщо D' - непарне, то $|S(a,D)|^2 = 0$.

Лему доведено.

Лема 1.2. Якщо D_1 і D_2 – взаємно прості додатні числа, то

$$S(aD_1, D_2) = S(aD_2, D_1) = S(a, D_1, D_2). \qquad (1.9)$$

Доведення:

$$\sum_{t_1} e^{2\pi i \cdot \frac{aD_1}{D_2} {t_1}^2} \cdot \sum_{t_1} e^{2\pi i \cdot \frac{aD_2}{D_1} {t_2}^2} = \sum_{t_1} \sum_{t_2} e^{2\pi i \cdot \frac{a\left({D_1}^2 {t_1}^2 + {D_2}^2 {t_2}^2\right)}{D_1 D_2}} =$$

$$= \sum_{t_1} \sum_{t_2} e^{2\pi i \cdot a(D_1 t_1 + D_2 t_2)^2}, \qquad (1.10)$$

де в сумах t_1 пробігає повну систему лишків за модулем D_2, а t_2 пробігає повну систему лишків за модулем D_1. При цьому $D_1 t_1 + D_2 t_2$ пробігає всю повну систему лишків за модулем $D_1 D_2$. Дійсно, всього членів в сумі $D_1 D_2$. Жодні два з них не порівняні між собою.

Дійсно, нехай

$$D_1 t_1 + D_2 t_2 \equiv D_1 {t_1}' + D_2 {t_2}' (mod\ D_1 D_2). \qquad (1.11)$$

Звідси

$$D_1(t_1 - {t_1}') \equiv 0(D_2), \quad D_2({t_2}' - t_2) \equiv 0(D_1). \qquad (1.12)$$

Але $(D_1, D_2) = 1$. Звідси

$$t_1 - {t_1}' \equiv 0(D_2), \quad {t_2}' - t_2 \equiv 0(D_1). \qquad (1.13)$$

Це протирічить припущенню.

Лема 1.3. Нехай p – просте непарне число, яке не ділиться на a. Тоді

$$\sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{ax^2}{\gamma}} = \left(\frac{a}{p}\right) \sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{x^2}{\gamma}}. \qquad (1.14)$$

Доведення:

$$\sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{ax^2}{p}} = 1 + \sum_{x=1}^{p-1} e^{2\pi i \cdot \frac{ax^2}{p}}. \qquad (1.15)$$

Якщо $\left(\frac{a}{p}\right) = 1$, то ax^2 пробігає той же клас лишків, що й x^2

$$\sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{ax^2}{p}} = 1 + \sum_{x=1}^{p-1} e^{2\pi i \cdot \frac{x^2}{p}} = \sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{x^2}{p}}. \quad (1.16)$$

Якщо $\left(\frac{a}{p}\right) = -1$, то ax^2 пробігає всі квадратичні нелишки, причому кожний з них два рази, а оскільки x^2 пробігає усі квадратичні лишки кожні два рази, то

$$\sum_{x=1}^{p-1} e^{2\pi i \cdot \frac{ax^2}{p}} + \sum_{x=1}^{p-1} e^{2\pi i \cdot \frac{x^2}{p}} = 2\sum_{x=1}^{p-1} e^{2\pi i \cdot \frac{x}{p}} = -2, \quad (1.17)$$

$$\sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{ax^2}{p}} = -\sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{x^2}{p}}. \qquad (1.18)$$

Лема 1.4. Якщо p – просте непарне число, то

$$\left(\sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{ax^2}{p}}\right)^2 = (-1)^{\frac{p-1}{2}} \cdot p. \qquad (1.19)$$

Доведення:

$$\sum_{x=0}^{p-1} e^{-2\pi i \cdot \frac{x^2}{p}} = \left(-\frac{1}{p}\right) \cdot \sum_{x=0}^{p-1} e^{2\pi i \cdot \frac{x^2}{p}}. \qquad (1.20)$$

Оскільки похідні спряжених величин дають квадрат модуля, то

$$\left|\sum_{x=0}^{p-1} e^{-2\pi i\cdot\frac{x^2}{p}}\right|^2 = (-1)^{\frac{p-1}{2}}\cdot\left(\sum_{x=0}^{p-1} e^{2\pi i\cdot\frac{x^2}{\gamma}}\right)^2; \quad (1.21)$$

$$p\cdot(-1)^{\frac{p-1}{2}} = \left(\sum_{x=0}^{p-1} e^{2\pi i\cdot\frac{x^2}{\gamma}}\right)^2. \quad (1.22)$$

Це доводить лему.

Лема 1.5. Якщо p та q – різні непарні прості числа, то

$$\left(\sum_{x=0}^{pq-1} e^{2\pi i\cdot\frac{x^2}{pq}}\right)^2 = (-1)^{\frac{pq-1}{2}}. \quad (1.23)$$

Доведення:

$$\sum_{x=0}^{pq-1} e^{-2\pi i\cdot\frac{x^2}{pq}} = \sum_{x=0}^{p-1} e^{-2\pi i\cdot\frac{qx^2}{p}}\cdot\sum_{x=0}^{q-1} e^{-2\pi i\cdot\frac{px^2}{q}} =$$

$$= \left(-\frac{q}{p}\right)\cdot\sum_{x=0}^{p-1} e^{2\pi i\cdot\frac{x^2}{p}}\cdot\left(-\frac{p}{q}\right)\sum_{x=0}^{q-1} e^{-2\pi i\cdot\frac{x^2}{q}} =$$

$$= (-1)^{\frac{p-1}{2}+\frac{q-1}{2}}\cdot\sum_{x=0}^{p-1} e^{2\pi i\cdot\frac{qx^2}{p}}\cdot\sum_{x=0}^{q-1} e^{2\pi i\cdot\frac{px^2}{q}} = (-1)^{\frac{p-1}{2}+\frac{q-1}{2}}\cdot\sum_{x=0}^{pq-1} e^{2\pi i\cdot\frac{x^2}{pq}} =$$

$$= (-1)^{\frac{pq-1}{2}}\cdot\sum_{x=0}^{pq-1} e^{2\pi i\cdot\frac{x^2}{pq}}. \quad (1.24)$$

або

$$\frac{p-1}{2}+\frac{q-1}{2} \equiv \frac{pq-1}{2}\ (mod\ 2). \quad (1.25)$$

Звідси:

$$\left|\sum_{x=0}^{pq-1} e^{-2\pi i\cdot\frac{x^2}{pq}}\right|^2 = (-1)^{\frac{pq-1}{2}}\cdot\left(\sum_{x=0}^{pq-1} e^{2\pi i\cdot\frac{x^2}{pq}}\right)^2, \quad (1.26)$$

що дає

$$(-1)^{\frac{pq-1}{2}} \cdot pq = \left(\sum_{x=0}^{pq-1} e^{2\pi i \cdot \frac{x^2}{pq}} \right)^2. \qquad (1.27)$$

Лема 1.6. Якщо D – додатнє непарне число, то

$$\sum_{x=0}^{4D-1} e^{2\pi i \cdot \frac{x^2}{4D}} = 2(1 + i^D) \cdot \sum_{x=0}^{D-1} e^{2\pi i \cdot \frac{x^2}{D}}. \qquad (1.28)$$

Доведення:

Оскільки D – *непарне число, то* $(D, 4) = 1$.

Тому

$$\sum_{x=0}^{3} e^{2\pi i \cdot \frac{Dx^2}{4}} \cdot \sum_{x=0}^{D-1} e^{2\pi i \cdot \frac{4x^2}{D}} = \sum_{x=0}^{4D-1} e^{2\pi i \cdot \frac{x^2}{4D}}. \qquad (1.29)$$

Але

$$\sum_{x=0}^{2} e^{2\pi i \cdot \frac{Dx^2}{4}} = 2(1 + i^D). \qquad (1.30)$$

Оскільки коли x пробігає повну систему лишків за модулем D, то і $2x$ пробігає повну систему лишків за модулем D.

Маємо

$$\sum_{x=0}^{D-1} e^{2\pi i \cdot \frac{4x^2}{D}} = \sum_{x=0}^{D-1} e^{2\pi i \cdot \frac{x^2}{D}}. \qquad (1.31)$$

Лема доведена.

Лема 1.7. Нехай a – непарне число, тоді

$$S(a, 2^r) = \sum_{x=0}^{2^r-1} e^{2\pi i \cdot \frac{x^2}{2^r}} = \begin{cases} 0, & \text{якщо } r = 1 \\ \left(1 + i^{\phi}\right) \cdot 2^{\frac{r}{2}}, & \text{якщо } r - \text{парне} \\ e^{2\pi i \cdot \frac{a}{b}} \cdot 2^{\frac{r+1}{2}}, & \text{якщо } r - \text{непарне}, r > 1. \end{cases} \qquad (1.32)$$

Доведення:

Справедливість формули при $r = 1,2,3$ перевіряємо безпосередньо.

Тепер нехай $r > 3$. Тоді $2(r-2) \geq r$.

$$\sum_{x=0}^{3} e^{2\pi i \cdot \frac{Dx^2}{4}} \cdot \sum_{x=0}^{D-1} e^{2\pi i \cdot \frac{4x^2}{D}} = \sum_{x=0}^{4D-1} e^{2\pi i \cdot \frac{x^2}{4D}}. \qquad (1.33)$$

$$\sum_{x=0}^{2^r-1} e^{2\pi i \cdot \frac{x^2}{2^r}} = \sum_{n=0}^{2^{r-2}-1} \sum_{t=0}^{3} e^{2\pi i \cdot \frac{a(2^{r-2}t+4)^2}{2^r}} = \sum_{n=0}^{2^{r-2}-1} e^{2\pi i \cdot \frac{an^2}{2^r}} \cdot \sum_{t=0}^{3} e^{2\pi i \cdot \frac{atn}{2}}. \quad (1.34)$$

Але

$$\sum_{t=0}^{3} e^{2\pi i \cdot \frac{atn}{2}} = \sum_{t=0}^{3} e^{2\pi i \cdot \frac{tn}{2}} = 2\sum_{t=0}^{1} e^{2\pi i \cdot \frac{tn}{2}} = \begin{cases} 0, \text{якщо } n - \text{непарне} \\ 4, \text{якщо } n - \text{парне} \end{cases}. \quad (1.35)$$

Це означає, що

$$\sum_{x=0}^{2^r-1} e^{2\pi i \cdot \frac{ax^2}{2^r}} = 4\sum_{n=0}^{2^{r-2}-1} e^{2\pi i \cdot \frac{an^2}{2^r}} = 4\sum_{t=0}^{2^{r-3}-1} e^{2\pi i \cdot \frac{at^2}{2^{r-2}}} =$$

$$= 2 \cdot \left(\sum_{t_1=0}^{2^{r-3}-1} e^{2\pi i \cdot \frac{at_1{}^2}{2^{r-2}}} + \sum_{t_2=0}^{2^{r-3}-1} e^{2\pi i \cdot \frac{a(t_2+2^{r-3})^2}{2^{r-2}}} \right) = 2 \cdot \sum_{t_1=0}^{2^{r-2}-1} e^{2\pi i \cdot \frac{at_1{}^2}{2^{r-2}}}. \quad (1.36)$$

Ми отримали суму того ж типу, з якої починали. Застосуємо тепер індукцію

$$\sum_{x=0}^{2^r-1} e^{2\pi i \cdot \frac{ax^2}{2^r}} = \begin{cases} 2^{\frac{r-2}{2}} \cdot \sum_{x=0}^{3} e^{2\pi i \cdot \frac{ax^2}{4}}, \text{для парного } r > 2, \\ 2^{\frac{r-3}{2}} \cdot \sum_{x=0}^{7} e^{2\pi i \cdot \frac{ax^2}{8}}, \text{для непарного } r > 3. \end{cases} \qquad (1.37)$$

Але нами уже помічено, що суми, які стоять у правих частинах даної рівності обчислюються.

Лему доведено.

Лема 1.8. Нехай a – непарне число, тоді

$$S(a,p^r)=\begin{cases} p^{\frac{r}{2}}, \text{для парного } r>2, \\ p^{\frac{r-1}{2}}\cdot S(a,p), \text{для непарного } r. \end{cases} \quad (1.38)$$

Доведення:

Для $r=1$ формулювання леми є тавтологією. Нехай $r>1$. Маємо:

$$\sum_{x=0}^{p^r-1} e^{2\pi i\cdot\frac{ax^2}{p^r}} = \sum_{n=0}^{p^{r-1}-1}\sum_{t=0}^{p-1} e^{2\pi i\cdot\frac{a(p^{r-1}\cdot t+n)^2}{p^r}} =$$

$$= \sum_{n=0}^{p^{r-1}-1} e^{2\pi i\cdot\frac{an^2}{p^r}}\cdot\sum_{t=0}^{p-1} e^{2\pi i\cdot\frac{2ant}{p^r}}. \quad (1.39)$$

Але $(2a,p)=1$. Тому внутрішня сума рівна

$$\sum_{t=0}^{p-1} e^{2\pi i\cdot\frac{2ant}{p}} = \begin{cases} 0, & n \text{ не ділиться на } p \\ p, & n \text{ ділиться на } p. \end{cases} \quad (1.40)$$

Це означає, що

$$S(a,p^r)=\text{р}\cdot\sum_{\substack{n=0 \\ n\equiv 0(mod\ p)}}^{p^r-1} e^{2\pi i\cdot\frac{an^2}{p^r}} = \text{р}\cdot\sum_{t=0}^{p^r-2} e^{2\pi i\cdot\frac{at^2}{p^{r-2}}}. \quad (1.41)$$

Таким чином,

$$S(a,p^r)=\text{р}\cdot S(a,p^{r-2}). \quad (1.42)$$

Зокрема $S(a,p^2)=\text{р}$.

Лему доведено.

Розділ 2. Точне значення суми Гауса

Чудово, що в сумі Гауса можна визначити не тільки модуль, а і її точне значення.

Теорема 2.1. Нехай $D = 4D'$, де D' - або просте число, або добуток двох непарних простих чисел

$$\sum_{x=0}^{D-1} e^{2\pi i \cdot \frac{x^2}{D}} = (1+i) \cdot \sqrt{D}, \qquad (2.1)$$

де корінь обирається зі знаком «+».

Доведення:

Передусім за лемою 6 та лемою 4 з попереднього розділу роботи маємо:

$$\left(\frac{1}{1+i} \cdot \sum_{x=0}^{4D'-1} e^{2\pi i \cdot \frac{x^2}{4D'}}\right)^2 = \left(\frac{2 \cdot (1+i^{D'})}{1+i}\right)^2 \cdot \left(\sum_{x=0}^{D'} e^{2\pi i \cdot \frac{x^2}{D'}}\right)^2 =$$

$$= 4D' \cdot \left(\frac{1+i^{D'}}{1+i}\right)^2 \cdot (-1)^{\frac{D'-1}{2}} = 4D' = D. \qquad (2.2)$$

Таким чином,

$$\frac{1}{1+i} \cdot \sum_{x=0}^{4D'-1} e^{2\pi i \cdot \frac{x^2}{4D'}} = \pm\sqrt{D}. \qquad (2.3)$$

є дійсним числом.

Покажемо, що

$$\frac{1}{1+i} \cdot \sum_{x=0}^{4D'-1} e^{2\pi i \cdot \frac{x^2}{4D'}} = \sqrt{D}. \qquad (2.4)$$

Виділимо в сумі члени з $x = 0$ та $x = 2D'$ та оскільки

$$e^{2\pi i \cdot \frac{(4D'-x)^2}{4D'}} = e^{2\pi i \cdot \frac{x^2}{4D'}}, \qquad (2.5)$$

то

$$\frac{1}{1+i}\cdot\sum_{x=0}^{4D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}=\frac{2+2\cdot\sum_{x=1}^{2D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}}{1+i}. \quad (2.6)$$

Виділимо в сумі члени з $x=D'$ та помітивши, що

$$e^{2\pi i\cdot\frac{(2D'-x)^2}{4D'}}=e^{2\pi i\cdot\frac{x^2}{4D'}}, \quad (2.7)$$

отримаємо

$$\frac{1}{2(1+i)}\cdot\sum_{x=0}^{4D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}=\frac{1+i^{D'}}{1+i}+2\cdot\frac{\sum_{x=1}^{D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}}{1+i}=$$

$$=\frac{(1-i)\cdot(1+i^{D'})}{2}+(1-i)\cdot\sum_{x=1}^{D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}. \quad (2.8)$$

Отже, потрібно визначити, що у рівності

$$\frac{(1-i)\cdot(1+i^{D'})}{2}+(1-i)\cdot\sum_{x=1}^{D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}=\pm D'^{\frac{1}{2}}. \quad (2.9)$$

стоїть знак «+».

Щоб визначити, який знак стоїть, розглянемо реальну частину.

При $D'\equiv 1\ (mod\ 4)$ $Re\frac{1}{2}\left(1+i^{D'}\right)(1-i)=1.$

При $D'\equiv 3\ (mod\ 4)$ $Re\frac{1}{2}\left(1+i^{D'}\right)(1-i)=0$

Маємо

$$Re\left[\frac{1}{2}\left(1+i^{D'}\right)(1-i)+(1-i)\cdot\sum_{x\le\sqrt{D'}}e^{2\pi i\cdot\frac{x^2}{4D'}}+(1-i)\cdot\sum_{\sqrt{D'}<x\le D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}\right]\ge$$

$$\ge Re\left[(1-i)\cdot\sum_{x\le\sqrt{D'}}e^{2\pi i\cdot\frac{x^2}{4D'}}+(1-i)\cdot\sum_{\sqrt{D'}<x\le D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}\right]\ge$$

$$\ge Re\left[(1-i)\cdot\sum_{x\le\sqrt{D'}}e^{2\pi i\cdot\frac{x^2}{4D'}}\right]-\sqrt{2}\cdot\left|\sum_{\sqrt{D'}<x\le D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}\right|. \quad (2.10)$$

Але

$$Re\left[(1-i)\cdot\sum_{x\le\sqrt{D'}}e^{2\pi i\cdot\frac{x^2}{4D'}}\right]=\sum_{x\le\sqrt{D'}}\left(\cos\frac{\pi x^2}{2D'}+\sin\frac{\pi x^2}{2D'}\right)\ge\left[\sqrt{D'}\right]\ge\frac{1}{2}\sqrt{D'}. \quad (2.11)$$

(оскільки $\cos\alpha+\sin\alpha\ge 1$ для $0\le\alpha\le\frac{\pi}{2}$).

Суму

$$\sum_{\sqrt{D'}<x\le D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}$$

будемо оцінювати по нерівності Кузьміна-Ландау.

Позначимо $l=\left[\sqrt{D'}\right]$, $f(x)=\ =\frac{x^2}{4D'}$, $\Delta f(x)=\frac{2x+1}{4D'}$ монотонно спадає і знаходиться між 0 та ½.

Звідси

$$\left|\sum_{l+1\le x\le D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}\right|\le\frac{1}{\sin\pi\,\Delta f(l+1)}+\frac{1}{\sin\pi\,\Delta f(D'-1)}=$$

$$=\frac{1}{\sin\pi\frac{2l+3}{4D'}}+\frac{1}{\sin\pi\frac{2D'-1}{4D'}}<\frac{2D'}{2l+3}+\frac{2D'}{2D'-1}<$$

$$<\frac{2D'}{2\sqrt{D'}+1}+\frac{2D'}{2D'-1}<\sqrt{D'}+\frac{6}{5}. \quad (2.12)$$

Тому

$$Re\left[\frac{1}{2}\left(1+i^{D'}\right)(1-i)+(1-i)\cdot\sum_{x\le\sqrt{D'}}e^{2\pi i\cdot\frac{x^2}{4D'}}+(1-i)\cdot\sum_{\sqrt{D'}<x\le D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}\right]\ge$$

$$\ge\left(\frac{1}{2}-\sqrt{2}\right)\cdot D'^{\frac{1}{2}}-\sqrt{2}\cdot\frac{6}{5}>-D'^{\frac{1}{2}}. \quad (2.13)$$

При $D\ge 10$ остання нерівність строга.

Тому

$$\frac{1}{2}\left(1+i^{D'}\right)(1-i)+(1-i)\cdot\sum_{x=1}^{D'-1}e^{2\pi i\cdot\frac{x^2}{4D'}}=D'^{\frac{1}{2}}, \qquad (2.14)$$

що й потрібно було довести.

Наслідок. Якщо D – просте непарне число або добуток двох простих непарних чисел, то

$$\sum_{x=0}^{D-1}e^{2\pi i\cdot\frac{x^2}{D}}=i^{\frac{1}{4}(D-1)^2}\cdot\sqrt{D}, \qquad (2.15)$$

де знак над коренем обирається з плюсом.

На основі попереднього розділу дослідження

$$\sum_{x=0}^{D-1}e^{2\pi i\cdot\frac{x^2}{D}}=\frac{1+i}{1+i^D}\cdot\sqrt{D}=i^{\frac{1}{4}(D-1)^2}\cdot\sqrt{D}. \qquad (2.16)$$

Відмітимо, що визначення знаку суми Гауса дає можливість довести квадратичний закон взаємності.

Теорема 2.2. Нехай p та q – два різних непарних числа. Справедлива рівність

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \qquad (2.17)$$

Доведення:

На основі наслідку з теореми 1 маємо

$$S(p,q)=i^{\frac{1}{4}(q-1)^2}\cdot\sqrt{q} \qquad (2.18)$$

$$S(q,p)=\frac{q}{r}i^{\frac{1}{4}(p-1)^2}\cdot\sqrt{r}. \qquad (2.19)$$

Далі за лемою 2.2 маємо:

$$S(1,pq)=S(p,q)\cdot S(q,p). \qquad (2.20)$$

Але

$$S(1,pq)=i^{\frac{1}{4}(pq-1)^2}\cdot\sqrt{pq}. \qquad (2.21)$$

Це нам дає:

$$\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right)\cdot i^{\frac{1}{4}((p-1)^2+(q-1)^2)}=i^{\frac{1}{4}(pq-1)^2}. \qquad (2.22)$$

Але

$$\frac{(pq-1)^2-(p-1)^2-(q-1)^2}{4}=\frac{p-1}{2}\cdot\frac{q-1}{2}\cdot\big((p+1)(q+1)-2\big). \qquad (2.23)$$

$$(p+1)(q+1)-2)\equiv 2\ (mod\ 4). \qquad (2.24)$$

Ми отримаємо:

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=i^{2\cdot\frac{p-1}{2}\cdot\frac{q-1}{2}}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \qquad (2.25)$$

Що і потрібно було довести.

Тепер «для порядку» доведемо наступне твердження.

Теорема 2.3. Нехай D – непарне число та $(a,D)=1$. Справедлива рівність

$$S(a,D)=\left(\frac{a}{D}\right)\cdot i^{\left(\frac{D-1}{2}\right)^2}\cdot\sqrt{D}. \qquad (2.26)$$

Доведення:

Для D = 1 відношення тривіалізується. Це означає, що можна вважати $D>1$.

Нехай $D=p^{2r}$, де p – просте непарне число.

Ми знаємо, що

$$S(a,p^{2r})=p^r. \qquad (2.27)$$

Далі

$$\left(\frac{a}{p^r}\right)\cdot i^{\left(\frac{p^{2r}-1}{2}\right)^2}\cdot\sqrt{p^{2r}}=\left(\frac{a}{p}\right)^{2r}\cdot p^r=p^r. \qquad (2.28)$$

(або $p^{2r}\equiv 1\ (mod\ 4)$).

Нехай $D=p^{2r-1}$, де p – просте непарне число. Ми бачили, що

$$S(a,p^{2r-1})=p^{r-1}\cdot S(a,p)=p^{r-1}\cdot\left(\frac{a}{p}\right)\cdot S(1,p)=$$

$$=p^{r-1}\cdot\left(\frac{a}{p}\right)\cdot i^{\left(\frac{p-1}{2}\right)^2}\cdot\sqrt{p}=\left(\frac{a}{p}\right)\cdot i^{\left(\frac{p-1}{2}\right)^2}\cdot\sqrt{p^{2r-1}} \qquad (2.29)$$

З іншого боку

$$\left(\frac{a}{p^{2r-1}}\right)\cdot i^{\left(\frac{p^{2r}-1}{2}\right)^2}\cdot\sqrt{p^{2r-1}}=\left(\frac{a}{p}\right)^{2r-1}\cdot i^{\left(\frac{p^{2r}-1}{2}\right)^2}\cdot\sqrt{p^{2r-1}}\ =$$

$$=\left(\frac{a}{p}\right)\cdot i^{\left(\frac{p^{2r}-1}{2}\right)^2}\cdot\sqrt{p^{2r-1}} \qquad (2.30)$$

Але

$$\left(\frac{p^{2r}-1}{2}\right)^2\equiv\left(\frac{p-1}{2}\right)^2\ (mod\ 4)\ (\text{або}\ p^{2r-1}\equiv p\ (mod\ 4)). \qquad (2.31)$$

Проведемо індукцію по числу різних простих множників D. Нехай $D=D_1\cdot D_2$, де $(D_1,D_2)=1$.

$$S(a,D_1D_2)=S(aD_2,D_1)\cdot S(aD_1,D_2)=\left(\frac{aD_2}{D_1}\right)\cdot i^{\left(\frac{D_1-1}{2}\right)^2}\cdot\sqrt{D_1}\cdot$$

$$\cdot\left(\frac{aD_1}{D_2}\right)\cdot i^{\left(\frac{D_2-1}{2}\right)^2}\cdot\sqrt{D_2}=\left(\frac{aD_2}{D_1}\right)\cdot\left(\frac{aD_1}{D_2}\right)\cdot i^{\frac{(D_1-1)^2+(D_2-1)^2}{4}}\cdot\sqrt{D_1D_2}, \qquad (2.32)$$

за припущенням індукції. За законом взаємності для символу Якобі

$$\left(\frac{aD_2}{D_1}\right)\cdot\left(\frac{aD_1}{D_2}\right)=\left(\frac{a}{D_1}\right)\cdot\left(\frac{a}{D_2}\right)\cdot\left(\frac{D_2}{D_1}\right)\cdot\left(\frac{D_1}{D_2}\right)=$$

$$=\left(\frac{a}{D_1D_2}\right)\cdot\left(\frac{D_2}{D_1}\right)\cdot\left(\frac{D_1}{D_2}\right)\cdot i^{\frac{D_1-1}{2}\cdot\frac{D_2-1}{2}}=\left(\frac{a}{D_1D_2}\right)\cdot i^{\frac{D_1-1}{2}\cdot\frac{D_2-1}{2}}. \qquad (2.33)$$

Це означає, що

$$S(a,D_1D_2)=\left(\frac{a}{D_1D_2}\right)\cdot i^{\frac{(D_1-1)^2+(D_2-1)^2+2(D_1-1)(D_2-1)}{4}}\cdot\sqrt{D_1D_2}. \qquad (2.34)$$

Але для усіх чотирьох комбінацій

$$D_1\equiv 1\ (mod\ 4),\qquad D_2\equiv 1\ (mod\ 4); \qquad (2.35)$$

$$D_1\equiv 1\ (mod\ 4),\qquad D_2\equiv 3\ (mod\ 4); \qquad (2.36)$$

$$D_1\equiv 3\ (mod\ 4),\qquad D_2\equiv 1\ (mod\ 4); \qquad (2.37)$$

$$D_1\equiv 3\ (mod\ 4),\qquad D_2\equiv 3\ (mod\ 4); \qquad (2.38)$$

перевіряється співвідношення

$$(D_1-1)^2+(D_2-1)^2+(D_1-1)(D_2-1)\equiv(D_1D_2-1)^2\ (mod\ 4), \qquad (2.39)$$

Таким чином,

$$S(a, D_1 D_2) = \left(\frac{a}{D_1 D_2}\right) \cdot i^{\left(\frac{D_1 D_2 - 1}{2}\right)^2} \cdot \sqrt{D_1 D_2}, \qquad (2.40)$$

що й потрібно було довести.

Розділ 3. Кватернарні суми Гауса

В ході нашого дослідження ми вивчили теорію сум Гауса над кінцевим полем Z_p. У цьому розділі розглядається узагальнення сум Гауса, а саме, ми вивчаємо кватернарні суми Гауса, які є узагальненням класичних сум Гауса.

Дослідження кватернарних сум Гауса має велике значення для розвитку сучасної математики. Вони дозволяють вирішувати складні проблеми, пов'язані зі структурою та властивостями чисел над кінцевими полями.

Нехай $q \geq 3$ – натуральне число, k – натуральне, a – ціле число. Сумою Гауса степеня k будемо називати суму

$$G(a;k;q) = \sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}} \qquad (3.1)$$

Для різних значень k багато авторів досліджували суми $G(a;k;q)$ і отримали цікаві результати (див. [2]-[7]).

Суттєвий вклад в теорію сум Гауса внесла робота Андре Вейля [9], в якій на основі доведення Вейлем гіпотези Рімана для алгебраїчних кривих над скінченним полем, мають обчислювати тригонометричні суми з многочленом в показнику, так для суми (1) можна довести оцінку

$$\left| \sum_{x \in Z_p^*} \chi(x) e^{2\pi i \frac{ax^k}{r}} \right| = \sum_{x=1}^{q} C(k)\sqrt{r},$$

$C(k)$ – стала, яка залежить тільки від k, (тут $\chi(x)$ – мультиплікативний характер зведеної системи лишків за модулем p).

Дослідженням кватернарних сум Гауса займались Вей Занг і Хайлян Ліу [2], які успішно отримали цікаві асимптотичні формули для розподілу значень $G(a;4;q)$. Завдяки їхнім результатам отримано більше розуміння про характеристики цих сум та їх властивості.

З іншого боку Янг і Тенг [3], вивчали проблему про кількість розв'язків конгруенції

$$x^2 + y^2 \equiv c(mod\ q), \qquad (x, y, q) = 1$$

і дали точну формулу.

В роботі П.Д. Варбанця [8] дослідив розподіл точок (x, y), які задовольняють конгруенцію

$$x^k \pm y^k \equiv a\ (mod\ p^m), \qquad k = 2{,}3$$

при умові, що точка (x, y) належить вузькому сектору одиничного кола:

$$x^k + y^k \leq x, |\arg(x + iy)| \leq \varphi,$$

де кут φ прямує до нуля, коли x прямує до нескінченності.

Нехай $S \in IN, p \equiv 1\ (mod\ 3), N_s$- кількість розв'язків рівняння

$$x_1^3 + x_2^3 + \cdots + x_s^3 = 0$$

над полем IF_r. Сарвадаман Чоула [4] довів, що $U_s = N_s - p^{s-1}$ задовольняють рекурентному співвідношенню

$$U_s = 3pU_{s-2} + pU_{s-3},$$

де

$$U_1 = 0, U_2 = 2p - 2, U_3 = (p - 1)d,$$

причому d однозначно визначається з умови $d^2 + 276^2, d \equiv 1\ (mod\ 3)$.

Пов'язані з цією роботою Човла результати можна знайти в роботах [5], [6,], [7].

У цій дипломній роботі ми вивчаємо величину $M_n(r)$, яка позначає кількість розв'язків конгруенції

$$x_1^4 + x_2^4 + \cdots + x_n^4 \equiv 0\ (mod\ p) \qquad (3.2)$$

за умови $0 \leq x \leq p - 1, i = 1, \dots, n$ (тут $r > 2$ – просте число).

Зауважимо, що за класичною теоремою Лагранжа кожне натуральне число можна зобразити сумою чотирьох квадратів цілих чисел, а для суми кубів достатньо 10 доданків виду y^3.

В цілому для кожного натурального k існує $s = s(k)$, так що кожне натуральне число N зображується сумою не більше s доданків k-ї степені натурального числа.

Це класична теорема Варніча, яка була доведена Іваном Матвійовичем Виноградовим майже 100 років тому.

Наша задача є аналогом теореми Варніча над скінченним полем Z_p.

В нашій роботі досліджується конгруенція (3.2) за допомогою сум Гауса $G(a; 4; q)$.

Нехай

$$D(r) := \sum_{x \leq Z_p^*} \left(\frac{x + x^{-1}}{p}\right),$$

де x^{-1} – означає мультиплікативне обернене для x (якщо $(x, \mathrm{p}) = 1$), а символ $\left(\frac{z}{p}\right)$, $(z, \mathrm{p}) = 1$) як завжди означає символ Лежандра.

Будуть доведені наступні теореми:

Теорема 3.1. Нехай $p = 8k + 5$ – просте число, $U_n(p) = M_n(p) - p^{n-1}$, тоді для кожного натурального $n \geq 5$ справедливе лінійне рекурсивне співвідношення 4-го порядку

$$U_n(p) = -2pU_{n-2}(p) + 4pBU_{n-1}(p) - (9p^3 - pB^2(p))U_{n-1}(p)$$

з ініціальними значеннями

$$U_1(p) = 0, U_2(p) = -(p-1), U_3(p) = 3(p-1)B(p),$$

$$U_4(p) = -7p(p-1) + (p-1)B_z(p).$$

Теорема 3.2. Нехай $p = 8k + 1$ – просте число, тоді для $n \geq 5$

$$U_n(p) = 6pU_{n-2}(p) + 4pBU_{n-3}(p) - (p^2 - p)B^2(p))U_{n-4}(p)$$

з ініціальними значеннями

$$U_1(p) = 0, U_2(p) = 3(p-1), U_3(p) = 3(p-1)B(p),$$

$$U_4(p) = 17p(p-1) + (p-1)B^2(p).$$

Допоміжні леми

Наступні леми, які є необхідними для доведення теорем 1 та 2 суттєво використовують матеріал першого розділу нашої роботи.

Лема 3.1. Нехай p – непарне просте число, $p \equiv 1\ (mod 4)$, тоді для кожного цілого b за умови $(b,p)=1$, справедливі тотожності

$$G(a;4;q)=\sum_{x=1}^{r-1} e^{2\pi i\frac{bx^4}{r}}=\left(\frac{b}{r}\right)\sqrt{p}+\sum_{x=1}^{r-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{r}} \qquad (3.3)$$

$$G^3(a;4;q)=R(p)\cdot p+\left(\frac{b}{r}\right)\sqrt{p}\left(\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{r}}\right)+\left(\frac{b}{r}\right)\sqrt{p}\sum_{x=1}^{r-1}\left(\frac{x+x^{-1}}{p}\right) \qquad (3.4)$$

де $R(p)=-1$, якщо $p=8k+5$ і $R(p)=3$, якщо $p=8k+1$.

Доведення. З властивостей символу Лежандра $\left(\frac{x}{p}\right)$ маємо

$$G(a;4;q)=\sum_{x=0}^{p-1} e^{2\pi i\frac{bx^4}{r}}=1+\sum_{a=1}^{p-1} e^{2\pi i\frac{bx^4}{p}}=1+\sum_{x=1}^{p-1}\left(1+\left(\frac{x}{p}\right)\right)e^{2\pi i\frac{bx^2}{p}}=$$

$$=\sum_{x=0}^{p-1} e^{2\pi i\frac{bx^2}{p}}+\sum_{x=1}^{p-1}\left(\frac{x}{r}\right)e^{2\pi i\frac{bx^2}{p}} \qquad (3.5)$$

З першого розділу нашої роботи маємо

$$\sum_{x=0}^{p-1} e^{2\pi i\frac{bx^2}{p}}=\left(\frac{b}{r}\right)\sum_{x=0}^{p-1} e^{2\pi i\frac{x^2}{p}}=\left(\frac{b}{p}\right)\sqrt{p} \qquad (3.6)$$

а тому формула (3.3) доведена.

З властивостей зведеної форми лишків за модулем p і формули (3.6) виводимо

$$\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{p}}\right)^2=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right)e^{2\pi i\frac{b(x^2+y^2)}{p}}=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\sum_{y=1}^{p-1} e^{2\pi i\frac{by^2(x^2+1)}{p}}=$$

$$=(p-1)\sum_{\substack{x=1\\ x^2+1\equiv 0\ (mod\ p)}}^{p-1}\left(\frac{x}{p}\right)+\sum_{\substack{y=1\\ (x^2+1,p)=1}}^{p-1}\left(\frac{x}{p}\right)\left(\sum_{y=0}^{p-1} e^{2\pi i\frac{y^2(x^2+1)}{p}}-1\right)=$$

$$= p \sum_{\substack{x=1 \\ x^2+1\equiv 0\ (mod\ p)}}^{p-1} \left(\frac{x}{p}\right) - \sum_{x=1}^{p-1}\left(\frac{x}{p}\right) + \left(\frac{b}{p}\right)\sqrt{p}\sum_{y=0}^{p-1} e^{2\pi i\frac{x(x^2+1)}{p}} =$$

$$= I(p)\cdot p + \left(\frac{b}{p}\right)\sqrt{p}\sum_{x=1}^{p-1}\left(e^{2\pi i\frac{x+x^{-1}}{p}}\right) \qquad (3.7)$$

де

$$I(p) = \begin{cases} -2, & \text{якщо } p = 8k+5 \\ 2, & \text{якщо } p = 8k+1 \end{cases}$$

З (5), (6) маємо тотожність.

$$G^2(a;4;q) = R(p)\cdot p + 2\left(\frac{b}{r}\right)\sqrt{p}\left(\sum_{\mathrm{x}=0}^{p-1}\left(\frac{\mathrm{x}}{r}\right)e^{2\pi i\frac{bx^2}{p}}\right) + \left(\frac{b}{r}\right)\sqrt{p}\sum_{x=1}^{r-1}\left(\frac{x+x^{-1}}{p}\right)$$

Це завершує доведення леми 3.1.

Аналогічно з (3.3) і (3.7) ми можемо довести, що для $p = 8k+1$:

$$G^3(a;4;q) = 7\left(\frac{b}{r}\right)\sqrt{p}\left(\sum_{x=1}^{p-1}\left(\frac{p}{r}\right)e^{2\pi i\frac{bx^2}{p}}\right) + 3p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) +$$

$$+\left(\frac{b}{r}\right)\sqrt{p}\left(\sum_{x=1}^{p-1}\left(\frac{x}{r}\right)e^{2\pi i\frac{bx^2}{p}}\right)\cdot\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) \qquad (3.8)$$

Для $p = 8k+5$:

$$G^3(a;4;q) = -5\left(\frac{b}{r}\right)p^{\frac{3}{2}} + p\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{p}}\right) + 3p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) +$$

$$+\left(\frac{b}{r}\right)\sqrt{p}\left(\sum_{x=1}^{p-1}\left(\frac{x}{r}\right)e^{2\pi i\frac{bx^2}{p}}\right)\cdot\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) \qquad (3.9)$$

Таким чином доведена лема.

Лема 3.2. В позначеннях теореми 1 маємо

$$G^3(a;4;q) = -5\left(\frac{b}{r}\right)p^{\frac{3}{2}} + p\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{p}}\right) + 3p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) +$$

$$+\left(\frac{b}{r}\right)\sqrt{p}\left(\sum_{x=1}^{p-1}\left(\frac{x}{r}\right)e^{2\pi i\frac{bx^2}{p}}\right)\cdot\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right).$$

Лема 3.3. Нехай p – непарне просте число, причому $p \equiv 1\ (mod 4)$, і нехай

$$N_k(p) = \sum_{k=1}^{p-1} A_k(b).$$

Тоді справедливі тотожності

$$N_1(p) = 0, N_2(p) = R(p)p(p-1), N_3(p) = 3p(p-1)\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right),$$

де $R(p) = -1$ для $p = 8k+5$, $R(p) = 3$ для $p = 8k+1$.

Доведення. В силу рівності

$$\sum_{x=0}^{r-1} e^{2\pi i\frac{ax}{r}} = \begin{cases} p, \text{якщо } a \equiv 0\ (mod\ 5) \\ 0, \text{інакше,} \end{cases} \qquad (3.10)$$

$\sum_{b=1}^{n-1}\left(\frac{b}{p}\right) = 0$ (тому що за модулем p кількість квадратичних лишків до рівнює кількості нелишків).

З леми 1 і властивості Гауса маємо

$$\sum_{b=1}^{p-1} G(b;4;p) = \sum_{b=1}^{p-1}\left(1 + \sum_{x=1}^{p-1} e^{2\pi i\frac{bx^2}{p}}\right) = p - 1 + \sum_{x=1}^{p-1}\sum_{b=1}^{p-1} e^{2\pi i\frac{bx^2}{p}} = 0 \quad (3.11)$$

Далі

$$\sum_{b=1}^{p-1} G^2(b;4;p) = \sum_{k=1}^{p-1} R(p)\cdot p + 2\sum_{b=1}^{p-1}\left(\frac{b}{p}\right)\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{p}}\right) +$$

$$+\sum_{b=1}^{p-1}\left(\frac{b}{r}\right)\sqrt{p}\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)=R(p)\cdot p(p-1)+$$

$$+2\sqrt{p}\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\sum_{b=1}^{p-1}\left(\frac{b}{p}\right)e^{2\pi i\frac{bx^2}{p}}=R(p)\cdot p(p-1)+$$

$$+2p\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)^3=R(p)\cdot p(p-1)+2p\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=R(p)\cdot p(p-1) \qquad (3.12)$$

Аналогічно (3.8) - (3.9) означають

$$\sum_{b=1}^{p-1}G^3(b;4;p)=3p(p-1)\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) \qquad (3.13)$$

Тут ми використали тотожність

$$\sum_{b=1}^{p-1}\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{p}}\right)=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\sum_{b=1}^{p-1}e^{2\pi i\frac{bx^2}{p}}=-\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=0.$$

Тепер Лема 3.3 випливає з (3.11) – (3.13).

Лема 3.4. Нехай p – непарне просте число, тоді

$$G^4(b;4;p)=\begin{cases}-2pG^2(b;4;p)+4pG(b;4;p)\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)-9p^2+\\ \quad+p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2, \text{якщо } p\equiv 5\ (mod\ 8);\\ 6pG^2(b;4;p)+4pG(b;4;p)\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)-p^2+\\ \quad+p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2, \text{якщо } p\equiv 1\ (mod\ 8);\end{cases}$$

Доведення. З (3.6) та леми 3.1 отримуємо

$$G^4(b;4;p) - R(p)pG^2(b;4;p) + R^2(p)p^2 = p\left(2\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{p}}\right) +$$

$$+\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2 = 4p\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{p}}\right)^2 +$$

$$+4p\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)e^{2\pi i\frac{bx^2}{p}}\right)\cdot\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) + p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2 =$$

$$= 4p\left(I(p)p + \frac{b}{p}\sqrt{p}\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) + p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2 \qquad (3.14)$$

Тепер з (3.14), означень $R(p)$ та $I(p)$ випливає, що для $p = 8k+5$

$$G^4(b;4;p) = -2pG^2(b;4;p) + 4pG(b;4;p)\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) -$$

$$-9p^2 + p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2 \qquad (3.15)$$

Для $p = 8k+1$

$$G^4(b;4;p) = 6pG^2(b;4;p) + 4pG(b;4;p)\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) -$$

$$-p^2 + p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2 \qquad (3.16)$$

Лема 3.4 випливає зі співвідношень (3.15) – (3.16).

Доведення теорем 3.1 та 3.2

Починаємо з доведення теореми 3.1.

Нехай $p \equiv 5\ (mod\ 5)$. Тоді для кожного натурального n з означення $M_n(p)$ і формули (3.1) маємо

$$M_n(p) = \sum_{\substack{x_1=0 \\ x_1{}^2+\cdots+x_4{}^2 \equiv 0\ (mod\ p)}}^{p-1} \ldots + \sum_{x_n=0}^{p-1} 1 = \frac{1}{p}\sum_{b=0}^{p-1}\left(\sum_{x=0}^{p-1} e^{2\pi i\frac{bx^4}{p}}\right)^n =$$

$$= p^{n-1} + \frac{1}{p}\sum_{b=1}^{p-1}\left(\sum_{x=0}^{p-1} e^{2\pi i\frac{bx^4}{p}}\right)^n = p^{n-1} + \frac{1}{p}\sum_{b=1}^{p-1}\left(\sum_{x=0}^{p-1} e^{2\pi i\frac{bx^4}{p}}\right)^n =$$

$$= p^{n-1} + \frac{1}{p}\sum_{b=1}^{p-1}\big(G(b;4;p)\big)^4. \qquad (3.17)$$

З (3.17) і леми 3.2 маємо

$$U_1(p) = M_1(p) - 1 = \frac{1}{p}\sum_{b=1}^{p-1} G(b;4;p) = 0 \qquad (3.18)$$

$$U_2(p) = M_2(p) - p = \frac{1}{p}\sum_{b=1}^{p-1} G^2(b;4;p) = -(p-1) \qquad (3.19)$$

$$U_3(p) = M_3(p) - p^2 = \frac{1}{p}\sum_{b=1}^{p-1} G^3(b;4;p) = 3(p-1)\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right) \qquad (3.20)$$

Лема 3.3 дає

$$U_4(p) = M_4(p) - p^3 = \frac{1}{p}\sum_{b=1}^{p-1} G^4(b;4;p) = -2pU_2(p) + 4pU_1(p)B(p) -$$

$$-(p-1)(9p - B(p)^2) = -7p(p-1) + (p-1)B(p)^2 \qquad (3.21)$$

Якщо $k \geq 5$, тоді з (3.17) і леми 3 маємо

$$U_k(p) = M_k(p) - p^{k-1} = \frac{1}{p}\sum_{b=1}^{p-1} G^k(b;4;p) = \frac{1}{p}\sum_{b=1}^{p-1} G^{k-4}(b;4;p) \times$$

$$\times(-2p)G^2(b;4;p)+4pG(b;4;p)\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)=$$

$$=-2pU_{k-2}(p)+4p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)U_{k-3}(p)-$$

$$-\left(9p^2-p\left(\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2\right)U_{k-4}(p)\right) \qquad (3.22)$$

З (3.18) – (3.22) випливає теорема 1.

Наслідок 3.1. Нехай $p=8k+3$ – просте число, тоді маємо

$$M_4(p)=p^3+(p-1)B(p)^2-7p(p-1)$$

$$M_5(p)=p^4-10p(p-1)B(p) \qquad (3.23)$$

Доведення теореми 3.2

Якщо $k\geq 5$, тоді з (3.17) і леми 3 маємо

$$U_k(p)=M_k(p)-p^{k-1}=\frac{1}{p}\sum_{b=1}^{p-1}G^k(b;4;p)=\frac{1}{p}\sum_{b=1}^{p-1}G^{k-4}(b;4;p)\cdot G^2(b;4;p)=$$

$$=6pU_{k-2}(p)+4p\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)U_{k-3}(p)-$$

$$-\left(p^2-p\left(\left(\sum_{x=1}^{p-1}\left(\frac{x+x^{-1}}{p}\right)\right)^2\right)U_{k-4}(p)\right) \qquad (3.24)$$

Тепер з (3.22) – (3.24) маємо твердження теореми 2.

Наслідок 3.2. Нехай $p\equiv 1\ (mod\ 8)$– просте число, тоді

$$M_4(p)=p^3+(p-1)B(p)^2+17p(p-1);$$

$$M_5(p)=p^4+30p(p-1)B(p). \qquad (3.25)$$

ВИСНОВКИ

Під час виконання роботи, мною було ретельно досліджено усі поставлені завдання, а саме: досліджено визначення та значення сум Гауса, сформульовано та доведено допоміжні леми, що потім були використані при доведенні основних теорем. В теоремах виведено рекурсивні співвідношення для $n \geq 5$ при $p = 8k + 5$ та $p = 8k + 1$, наведено наслідки з них.

Також у дипломній роботі сформульовано та доведено основні леми теорії сум Гауса, а також досліджено основні питання точного значення сум Гауса.

Крім того, в роботі розглядається узагальнення сум Гауса, а саме кватернарні суми.

СПИСОК ВИКОРИСТАНИХ ДЖЕЛЕЛ

1. Дэвенпорт Г., Мультипликативная теория чисел, М. Наука, 1971.
2. Zhang W., Liu H., On the general Gauss sums and their fourth power mean, Osaka I., Math. 2005, v.42, 189 - 199.
3. Yang Q., Tang M., On the addition of squares of units and nonunits modulo n., J Numbers Theory. 2015, v.155, 1 - 12.
4. Chowla S., Chowla M., On the number zeros of diagonal cubic forms, J Numbers Theory. 1977, v.9, 502 - 506.
5. Sander I., On the addition of units and nonunits mod m, J. Number Theory. 2009, v. 129, 2260-2266.
6. Cohen S., Zhang W., Sums of two exact powers, Finite Fields and Their Applications, 2002, v.8, 471 - 477.
7. Apostol T., Zhang W., The introduction to Analytic Number Theory. 1976, Springer, NY.
8. Варбанец П. Д. Проблемы круга в арифметической прогрессии. Математические заметки, 1970, 6, 173 – 192.
9. Weil A., On some exponential sums, Proc Natl Acad Sci USA, 1948, v.34, 204 - 207.
10. Shen S., Zhang W., On the quartic Gauss sums, On the quartic Gauss sums, Advances in Different Equations, 2017, v.43, 1 - 9.