Одеський національний університет імені І. І. Мечникова

Факультет математики, фізики та інформаційних технологій

Кафедра алгебри, геометрії та диференціальних рівнянь

Кваліфікаційна робота

на здобуття ступеня вищої освіти «магістр»

«Теорія порівнянь по модулю ступеня простого числа»

«Prime power congruence theory»

Виконав: здобувач денної форми навчання
спеціальності 111 Математика
Освітня програма «Математика»
Клішин Микита Євгенович

Керівник: доктор фіз.-мат. наук, проф. Варбанець П. Д. ___
Рецензент: канд. фіз.-мат. наук, доц. Бєлозьоров Г. С.

Рекомендовано до захисту:

Протокол засідання кафедри

№ ___ від _____ 2023 р.

Завідувач кафедри

_____ _____

Захищено на засіданні ЕК № _____

Протокол № ___ від _____ 2023 р.

Оцінка _____ / _____ / _____

Голова ЕК

_____ _____

Одеса — 2023 р.

ЗМІСТ

ВСТУП

Роботу присвячено дослідженню методом тригонометричних сум ряда конгруецій з метою виведення асимптотичних формул кількості їхніх розв'язків.

Актуальність. Проблемою дослідження кількості розв'язків конгруенцій, на початку XX століття, займалися такі видатні вчені як І. М. Виноградов , Х. Клостерман, Г. Давенпорт, Х. Хасе і Г. Вейль. В період другої половини XX століття можна відзначити таких науковців, як Л. Мордел, К. Хулі, Л. П. Постнікова, П. Д. Варбанець та С. А. Степанов.

При розв'язанні подібних задач найчастіше використовуєьться метод тригонометричних сум, який був запропонований і розроблений І. М. Виноградовим. Також використовують оцінки тригонометричних сум.

Кількість розв'язків конгруенцій є основним елементом теорії чисел та аналітичної теорії чисел. Вивчення якого допомагає зрозуміти властивості чисел та їх взаємозв'язки.

Кількість розв'язків конгруенцій та їх розподіл має практичне застосування в криптографії, особливо в алгоритмах шифрування на основі конгруенцій. Зокрема дослідження розв'язків конгруенцій виду $y^2 \equiv x^3 + ax + b \ (mod\ p^n)$ дає результати для криптографії на еліптичних кривих над скінченним кільцем (у випадку $mod\ p$ – над скінченним полем). Знання про розподіл розв'язків може допомогти в розробці та вдосконаленні криптографічних систем, зокрема завдяки цьому з'являється можливість генерувати послідовності псевдо-випадкових чисел.

Мета роботи

Метою моєї роботи є застосування методу тригонометричних сум та методів Л.П. Постнікової для дослідження кількості розв'язків і узагальнення

відомостей ряду конгруенцій:

$$y^2 \equiv x^3 + a \ (mod\ p^n) \tag{0.1}$$

$$y^2 \equiv x^3 + ax + b \ (mod\ p^n) \tag{0.2}$$

$$y^2 \equiv x^4 + x^2 + a \ (mod\ p^n) \tag{0.3}$$

$$x^s + y^m \equiv 1 \ (mod\ p^n) \tag{0.4}$$

Структура роботи. Дипломна робота складається зі вступу, двох розділів, висновку та списку літератури.

У першому розділі розглянуто метод Мордела оцінки кількості розв'язків конгруецій та наведено приклад застосування його методу. Також наведені необхідні теореми та попередні результати.

У другому розділі наведені отримані уявлення для розв'язків виду для конгруенцій (0.1) – (0.4). Також наведені способи оцінювання тригонометричних сум, які виникають при розв'язанні задачі про кількість розв'язків конгруенцій.

РОЗДІЛ 1

ПОПЕРЕДНІ РЕЗУЛЬТАТИ

1.1 Оцінка для кількості розв'язків m конгруенцій за модулем p

Нехай p просте число, $\xi = (\xi_1, \ldots, \xi_n)$ n цілих змінних і $f(\xi), f_1(\xi), \ldots, f_m(\xi)$ $m+1$ многочлен від ξ з цілими коефіцієнтами. Нехай $l = (l_1, \ldots, l_n)$ n заданих цілих чисел, які задовольняють умовам $0 \le l_1 < p, \ldots, 0 \le l_n < p$, або іншими словами $0 \le (l) < p$. Розглянемо дві задачі.

Перша задача це пошук оцінки для тригонометричної суми

$$S'_n = \sum_{\xi} e(f(\xi_1, \ldots, \xi_n)),\ 0 \le \xi_1 < l_1, \ldots, \xi_n < l_n, \tag{1.1}$$

іншими словами $0 \le (\xi) < (l)$, де $e(x) = \exp\left(\dfrac{2\pi i x}{p}\right)$, в термінах повних тригонометричних сум

$$S'_n = \sum_{x} e(f(x_1, \ldots, x_n)),\ 0 \le (x) < p \tag{1.2}$$

Друга задача – знайти оцінку кількості розв'язків $N'_{n,m}$ m когруенцій за модулем p

$$f_1(\xi) \equiv 0, \ldots, f_m(\xi) \equiv 0,\ 0 \le (\xi) < (l) \tag{1.3}$$

в термінах кількості розв'язків $N_{n,m}$

$$f_1(x) \equiv 0, \ldots, f_m(x) \equiv 0,\ 0 \le (x) < p \tag{1.4}$$

Тут і далі будемо вважати, що всі змінні позначені латинськими літерами набувають значень 0, 1, $\ldots$, $p-1$. Змінні ξ_1, $\xi_2, \ldots$ набувають значень 0, 1, $\ldots$, $l_1 - 1$.

Відносно першої задачі відомі доведення і результат, для випадку $n = 1$, запишемо у іншому вигляді, який дає уявлення для узагальненя цього результату для довільного n, і дає ідею для другої задачі.

Припустимо, що $n = 1$, $\xi = \xi_1$, тоді

$$S_1' = \sum_{\xi} e(f(\xi)),\ 0 \le \xi < l.$$

Очевидно, що

$$pS_1' = \sum_{x,t,\xi} e(f(x) + t(x - \xi)). \tag{1.5}$$

Сумуючи по t отримуємо нуль, хіба що $x = \xi$, коли отримуємо дільник p.

Далі сумуємо відносно ξ. Доданок при $t = 0$ має вигляд $l \sum_x e(f(x)) = lS_1$. Коли $t \ne 0$, при сумуванні відносно ξ, отримуємо

$$\sum_{x,t>0} e(-t\xi) = \frac{1 - e(-tl)}{1 - e(-t)}$$

так, що

$$pS_1' = lS_1 + \sum_{x,t>0} e(f(x) + tx)\frac{1 - e(-tl)}{1 - e(-t)} \tag{1.6}$$

Припустимо далі, що ми маємо наступну незалежну від t оцінку

$$\left| \sum_x e(f(x) + tx) \right| \le E. \tag{1.7}$$

Легко бачити, що

$$|pS_1' - lS_1| \le E \sum_{t>0} \left(\frac{\sin \pi t}{p} \right)^{-1} \le Ep \log p.$$

Отже, отримуємо добре відомий результат:

$$S_1' = lp^{-1} S_1 + \Theta E \log p,\ |\Theta| < 1$$

Далі розглянемо випадок для довільного n з $\xi = (\xi_1, \ldots, \xi_n)$, $l = (l_1, \ldots, l_n)$, $x = (x_1, \ldots, x_n)$ і $\xi_i < l_i$, $i = \overline{1,n}$.

Маємо

$$S_n' = \sum_{\xi} e(f(\xi)),\ S_n = \sum_{x} e(f(x)). \tag{1.8}$$

Припускаємо, що існують оцінки $E_n^{(0)}, E_n^{(1)}, \ldots, E_n^{(n)}$, які незалежні від t, і такі, що

$$\left| \sum_{x} e(f(x) + t \cdot x) \right| \le E_n^{(r)}, \tag{1.9}$$

де $t \cdot x = \sum_{j=1}^{n} t_j x_j$ і r - число ненульових t. Таким чином $E_n^{(0)} = |S_n|$. Зазвичай оцінки $E_n^{(r)}$ можуть бути замінені на незалежну від r оцінку E_n, але іноді може бути корисним зберегти $E_n^{(r)}$. Тоді значення $E_n^{(r)}$ залежатиме від того, які r з t не дорівнюють нулю і тоді сумування по r міститиме всі варіанти t які дорівнюютю нулю.

Доводимо, що

$$S_n' = l_1 \ldots l_n p^{-n} S_n + \Theta_n^{(n)} E_n^{(n)} (\log p)^n + R_n,\ |\Theta_n^{(n)}| < 1, \tag{1.10}$$

де за домовленістю про сумування відносно r отримаємо

$$R_n = \sum_{r=1}^{n-1} \Theta_n^{(r)} l_{r+1} \ldots l_n p^{r-n} E_n^{(r)} (\log p)^r,\ |\Theta_n^{(n)}| < 1. \tag{1.11}$$

Доведення аналогічне випадку при $n = 1$. Таким чином

$$p^n S'_n = \sum_{x,t,\xi} e(f(x) + t \cdot (x - \xi)). \tag{1.12}$$

Очевидно сумування по t дає нуль, хіба що $x = \xi$ коли ми отримуємо $p^n S'_n$. Коли всі t дорівнюють нулю в (1.12) маємо внесок $l_1 l_2 \dots l_n S_n$. Припустимо, що r з t не дорівнюють нулю. Для зручності нехай $t_1, \dots, t_r$ не дорівнюють нулю, а $t_{r+1}, \dots, t_n$ всі дорівнюють нулю. Результат сумування по ξ

$$l_{r+1} \dots l_n \sum_{t,x} e(f(x) + t \cdot x) \frac{1 - e(-l_1 t_1)}{1 - e(-t_1)} \dots \frac{1 - e(-l_r t_r)}{1 - e(-t_r)}.$$

Цей результат за модулем не перевищує

$$l_{r+1} \dots l_n \sum_t E_n^{(r)} \left(\sin \frac{\pi t_1}{p} \dots \sin \frac{\pi t_r}{p} \right)^{-1} < l_{r+1} \dots l_n E_n^{(r)} p^r (\log p)^r.$$

Сумуючи по r і позначаючи через $\Theta_n^{(r)}$ такі доданки, що $|\Theta_n^{(r)}| < 1$, отримуємо значення R_n з (1.11)

Таким чином ми підійшли до другої задачі. Позначимо через $N'_{n,m}$ кількість розв'язків конгруенцій

$$f_j(\xi) \equiv 0,\ 0 \le (\xi) < (l)\ (j = 1, \dots, m), \tag{1.13}$$

та через $N_{n,m}$ кількість розв'язків конгруенцій

$$f_j(x) \equiv 0,\ 0 \le (x) < p\ (j = 1, \dots, m), \tag{1.14}$$

Якщо ми покладемо $u \cdot f(x) = u_1 f_1(x) + \dots + u_m f_m(x)$, то отримаємо

$$p^{n+m} N'_{n,m} = \sum_{u,t,x,\xi} e\left(u \cdot f(x) + t \cdot (x - \xi)\right), \tag{1.15}$$

оскільки сума відносно t і u дорівнює нулю, хіба що $x = \xi, f_j(\xi) \equiv 0 (j = 1, \ldots, m)$. Ми будемо вимагати деяких оцінок для тригонометричних сум, незалежних, в свою чергу, від t і u. Припустимо, що

$$\left| \sum_{x,u} e\left(u \cdot f(x) + t \cdot x\right) \right| \leq E_n^{(r)}, \tag{1.16}$$

де r означає кількість t, які не дорівнюють нулю. Іноді оцінка $E_n^{(r)}$ може бути заминена на незалежну від r оцінку E_n, але згодом стає зрозуміло, зо зручніше залишити $E_n^{(r)}$. Зауважимо, як і раніше, що значення $E_n^{(r)}$ буде залежати від вибору r з t, які не дорівнюють нулю, і що підсумовування r включає всі вибрані.

Ми доводимо, що

$$N'_{n,m} = l_1 \ldots l_n p^{-n} N_{n,m} + \Theta E_n^{(n)} (\log p)^n + R_n, \tag{1.17}$$

де

$$R_n = \sum_{r=1}^{n-1} \Theta_n^{(t)} l_{r+1} \ldots l_n p^{r-n-m} (\log p)^r E_n^{(r)} \tag{1.18}$$

з угодою на сумування по r і $|\Theta_n^{(r)}| < 1$.

Коли всі t дорівнюють нулю в (1.15), отримуємо внесок $p^m l_1 \ldots l_n N_{n,m}$. Припустимо що r із t не дорівнюють нулю $t_1, \ldots, t_r$. Тоді так само як в (1.12), маємо внесок $\Theta_n^{(r)} l_{r+1} \ldots l_n p^{r-n} E_n^{(r)} (\log p)^r$, а отже виконуються (1.17) і(1.18).

Оцінка (1.17) залежить від пошуку корисних оцінок для $E_n^{(r)}$. Грубі оцінки для сумування по x досить легко знайти але тоді сумування по u дає дільник p. Більш точні результати можна отримати, якщо використати аналітичний вид виразу для суми по x. Для простоти розглянемо два випадки, коли $m = 1$ і $f(x)$ є загальним квадратичним многочленом від x:

$$f(x) = a_1 x_1^2 + \cdots + a_n x_n^2 + a, \; a_1 \ldots a_n \not\equiv 0 \tag{1.19}$$

$$a_1x_1^2+\cdots+a_sx_s^2+a_{s+1}x_{s+1}+\cdots+a_nx_n+a,\ a_1\ldots a_n\not\equiv 0 \qquad (1.20)$$

В першому випадку загальна тригонометрична сума (1.16) набуває вигляду

$$E=\sum_{x,u} e\left(u\left(a_1x_1^2+\cdots+a_nx_n^2+a\right)+t_1x_1+\cdots+t_nx_n\right). \qquad (1.21)$$

Припустимо на початку, що всі t дорівнюють нулю. Тоді маємо $E'=pl_1\ldots l_nN_{n,1}$, де $N_{n,1}$ число розв'язків конгруенції

$$a_1x_1^2+\cdots+a_nx_n^2+a\equiv 0.$$

Тоді

$$pN_{n,1}=\sum_{u,x} e\left(u\left(a_1x_1^2+\cdots+a_nx_n^2+a\right)\right)=$$
$$=p^n+\sum_{u=1,x=0}^{p-1} e\left(u\left(a_1x_1^2+\cdots+a_nx_n^2+a\right)\right)=$$
$$=p^n+i^{n(p-1/2)^2}\left(\frac{a_1\ldots a_n}{p}\right)p^{n/2}\sum_{u=1}^{p-1}\left(\frac{u}{p}\right)e\left(au\right),$$

і тому легко оцінюється. Оскільки результат добре відомий, його достатньо буде процитувати $p\neq 2$.

Припустимо n парне.

Якщо $a\not\equiv 0$, то $N_{n,1}=p^{n-1}-\left(\dfrac{(-1)^{n/2}a_1\ldots a_n}{p}\right)p^{(n-2)/2}$

Якщо $a\equiv 0$, то $N_{n,1}=p^{n-1}-(p-1)\left(\dfrac{(-1)^{n/2}a_1\ldots a_n}{p}\right)p^{(n-2)/2}$

Припустимо n непарне.

Якщо $a \not\equiv 0$, то $N_{n,1} = p^{n-1} + \left(\dfrac{(-1)^{(n+1)/2} a a_1 \dots a_n}{p}\right) p^{(n-1)/2}$

Якщо $a \equiv 0$, то $N_{n,1} = p^{n-1}$.

Припустимо далі, що всі t не дорівнюють нулю. Тоді сума в (1.21) з $u = 0$ дорівнює нулю і тому ми можемо припустити далі, що $u \neq 0$.

Суми по x є Гаусовими сумами і тому ми маємо внесок

$$E' = i^{n((p-1/2))^2} p^{n/2} \left(\frac{a_1 \dots a_n}{p}\right) {\sum_u}' \left(\frac{u^n}{p}\right) e\left(au - \frac{t_1^2}{4a_1 u} \cdots - \frac{t_n^2}{4a_n u}\right), \tag{1.22}$$

де $1/4a_1 u = u'$ з $4a_1 u u' \equiv 1$

Далі розглянемо суми

$$K_{c,d}^{(n)} = {\sum_u}' \left(\frac{u^n}{p}\right) e\left(cu + \frac{d}{u}\right)$$

де $\dfrac{1}{u} = u'$ і $uu' \equiv 1$. При парному n маємо суми Клостермана. Якщо $cd \equiv 0$, $K_{c,d}^{(n)} = -1$, якщо не викнується $c \equiv d \equiv 0$, то $K_{c,d}^{(n)} = p - 1$. У випадку $cd \not\equiv 0$ маємо оцінку Вейля

$$\left|K_{c,d}^{(0)}\right| \leq 2\sqrt{p},$$

і цю оцінку також можна використовувати, якщо не виконується $c \equiv d \equiv 0$.

Для випадку непарного n доведено, що $K_{c,d}^{(1)}$ може бути виражене через скінченну кількість доданків. Для наших цілей досить сказати, що $\left|K_{c,d}^{(1)}\right| \leq 2\sqrt{p}$. Отже в (1.17), (1.18) ми можемо взяти $E_n^{(r)} = O(p^{(n+1)/2})$

Далі розглянемо другий випадок квадриточної форми приведеної в

(1.20). Тригонометрична сума в (1.16) набуде наступного вигляду

$$E = \sum_{x,u} e(g(x,u)), \tag{1.23}$$

де

$$g(x,u) = u(a_1x_1^2+\cdots+a_sx_s^2+a_{s+1}x_{s+1}+\cdots+a_nx_n+a)+t_1x_1+\cdots+t_nx_n. \tag{1.24}$$

Коли всі t дорівнюють нулю, маємо внесок p^n в E, оскільки

$$a_1x_1^2 + \cdots + a_sx_s^2 + a_{s+1}x_{s+1} + \cdots + a_nx_n + a \equiv 0$$

має p^{n-1} розв'язків.

Припустимо, що всі t не дорівнюють нулю. Тоді внесок в E, при $u = 0$, дорівнює нулю, а отже ми можемо припустити далі, що $u \neq 0$. При $x_1, \ldots, x_s$ суми є Гаусовськими, а отже

$$E' = i^{s((p-1)/2)^2}p^{s/2}\left(\frac{a_1 \ldots a_s}{p}\right)\sum_{x,u}\left(\frac{u}{p}\right)^s e(h(x,u)),$$

де

$$h(x,u) = x_{s+1}(a_{s+1}u + t_{s+1}) + \cdots + x_n(a_nu + t_n) + au - \frac{t_1^2}{4a_1u} - \cdots - \frac{t_s^2}{4a_su}.$$

При $x_{s+1}, \ldots, x_n$ суми дорівнюють нулю, якщо не виконуються

$$a_{s+1}u + t_{s+1} = 0, \ldots, a_nu + t_n = 0.$$

Це дає щонайбільше одне значення u. Отже

$$|E'| \leq p^{s/2}p^{n-s} = p^{n-s/2}. \tag{1.25}$$

Цей результат може бути використаним в (1.17) і (1.18) для всіх $E_n^{(r)}$.

Розглянемо випадок m конгруенцій від n змінних,

$$f_j(\xi) \equiv 0,\ 0 \le (\xi) < (l),\ j = 1, \ldots, m.$$

Ми вже побачили, що кількість розв'язків $N'_{n,m}$ визначається наступною рівністю

$$N'_{n,m} = l_1 \ldots l_n p^{-n} N_{n,m} + \Theta_n^{(n)} (\log p)^n E_n^{(n)} + R_n, \tag{1.26}$$

де

$$R_n = \sum_{r=1}^{n-1} \Theta_n^{(r)} l_{r+1} \ldots l_n p^{r-n-m} (\log p)^r E_n^{(r)} \tag{1.27}$$

Кількість розв'язків $N_{n,m}$ визначається рівністю

$$p^m N_{n,m} = \sum_{x,u} e\left(\sum_{s=1}^{m} u_s f_s(x) \right). \tag{1.28}$$

Доданки з усіма $u \equiv 0$ вносять p^n до суми, тому припустимо далі, що всі $u \not\equiv 0$. У деяких ситуаціях може бути бажано розглянути різні випадки, коли деякі з $u \equiv 0$. Але такої потреби немає, коли всі $f(x)$ є квадратичними формами наступного вигляду

$$f_s(x) = a_{s,1} x_1^2 + \cdots + a_{s,n} x_n^2 + a_s. \tag{1.29}$$

Сумування в (1.28) набуває вигляду

$$S = \sum_{u,x} e(h(x,u)), \tag{1.30}$$

де

$$h(x,u) = \sum_{s=1}^{n} \left(\sum_{t=1}^{m} (u_t a_{ts}) x_s^2 + \sum_{t=1}^{m} u_t a_t \right) \tag{1.31}$$

Припустимо u такий, що жоден x^2 не має коефіцієнта конгруентного нулю. Суми відносно x є Гаусовими і тому є внесок S' в (1.30), наступного

виду

$$S' = i^{n((p-1)/2)^2} p^{n/2} \sum_u \prod_{s=1}^{n} \left(\frac{u_1 a_{1s} + \cdots + u_m a_{ms}}{p} \right) e(u_1 a_1 + \cdots + u_m a_m). \tag{1.32}$$

Припустимо далі, що r серед x^2 мають коефіцієнти конгруентні нулю. Підсумовування по цим x дає p^r. Тоді, замінивши r з u через решту $n-r$ з u, ми отримаємо суму, подібну до (1.32). Знаходження точної оцінки для (1.32) є досить складною задачею, навіть при використанні оцінки Вейля.

Особливий випадок $m = 2$, $a_1 = a_2 = 0$ вартий уваги. (1.32) набуде вигляду

$$S' = i^{n((p-1)/2)^2} p^{n/2} \sum_u \prod_{s=1}^{n} \left(\frac{u_1 a_{1s} + u_2 a_{2s}}{p} \right)$$

Внесок при $u_2 \equiv 0$

$$\sum_{u_1} \left(\frac{u_1^n}{p} \right) \left(\frac{a_1 1 \dots a_{1n}}{p} \right) = 0, \text{якщо } n \text{ парне},$$

$$\sum_{u_1} \left(\frac{u_1^n}{p} \right) \left(\frac{a_1 1 \dots a_{1n}}{p} \right) = (p-1) \left(\frac{a_1 1 \dots a_{1n}}{p} \right) \text{ якщо } n \text{ непарне}.$$

Коли $u_2 \not\equiv 0$, покладемо $u_1 = u u_2$. Внесок в S'

$$i^{n((p-1)/2)^2} p^{n/2} \sum_{u,u_2} \left(\frac{u_2}{p} \right)^n \prod_{s=1}^{n} \left(\frac{u_1 a_{1s} + u_2 a_{2s}}{p} \right) = 0 \text{ якщо } n \text{ парне},$$

$$i^{n((p-1)/2)^2} p^{n/2} \sum_{u,u_2} \left(\frac{u_2}{p} \right)^n \prod_{s=1}^{n} \left(\frac{u_1 a_{1s} + u_2 a_{2s}}{p} \right) = O((p-1)p^{(n+3)/2})$$

якщо n непарне,

оскільки кількість розв'язків конгруенції

$$v^2 \equiv \prod_{s=1}^{n} \left(\frac{ua_{1s} + a_{2s}}{p} \right)$$

дорівнює $p + O(\sqrt{p})$ за теоремою Вейля.

Розглянемо наступний випадок в (1.31), коли деякі з x^2 мають коефіцієнти конгруентні нулю. Для простоти припустимо, що це виконується тільки для одного коефіцієнта, і тому a обов'язково задовольняє умову $\frac{a_{1,\lambda}}{a_{2,\lambda}} \not\equiv \frac{a_{1,\mu}}{a_{2,\mu}}$ для всіх $\lambda \neq \mu$, $1 \leq \lambda, \mu \leq n$. Досить розглянути випадок коли x_1^2 має коефіцієнт конгруентний нулю. Тоді $u_1 a_{11} + u_2 a_{21} \equiv 0$ і внесок в (1.31) набуває форми

$$S'' = i^{(n-1)((p-1)/2)^2} p^{(n+1)/2} \sum_{u} \prod_{s=2}^{n} \left(\frac{u_1 a_{1s} + u_2 a_{2s}}{p} \right).$$

Покладемо $u_1 = t a_{21}$, $u_2 = -t a_{11}$. Тоді

$$S'' = i^{(n-1)((p-1)/2)^2} p^{(n+1)/2} \sum_{t} \left(\frac{t}{p} \right)^{n-1} \prod_{s=2}^{n} \left(\frac{a_{21}a_{1s} + a_{11}a_{2s}}{p} \right) = 0$$

якщо n парне,

$$S'' = i^{(n-1)((p-1)/2)^2} p^{(n+1)/2} \sum_{t} \left(\frac{t}{p} \right)^{n-1} \prod_{s=2}^{n} \left(\frac{a_{21}a_{1s} + a_{11}a_{2s}}{p} \right) = O(p^{(n+3)/2})$$

якщо n непарне.

Тоді з (1.28) отримуємо

$$p^2 N_{n,2} = p^n + O(p^{(n+3)/2}) \implies N_{n,2} = p^{n-2} + O(p^{n-1}/2).$$

1.2 Застосування метода Мордела

В позначеннях попереднього розділу розглянемо задачу пошуку оцінки N'_m через N_m.

Маємо

$$p^{(m+-1)n}N'_m = \sum_{u=0}^{p^n-1}\sum_{(t)=0}^{p^n-1}\sum_{(x)=0}^{p^n-1}\sum_{(\xi)=0}^{(l)} e^{2\pi i(uf(x)+t\cdot(x-\xi))/p^n} \tag{1.33}$$

Сумування по t і u дає нуль, крім випадку, коли $x = \xi$, $f(\xi) \equiv 0(mod\ p^n)$.

Припустимо, що ми маємо оцінки для тригонометричних сум, які не залежать від t:

$$\left|\sum_{u}\sum_{(x)} e^{2\pi i(uf(x)+t\cdot(x-\xi))/p^n}\right| \leq E_m^{(r)}, \tag{1.34}$$

де r - кількість ненульових координат вектора t.

Покажемо, що

$$N'_m = l_1 \dots l_m p^{-mn} N_n + \Theta_m^{(m)} E_m^{(m)} p^{-n} \log^m p^n + R_m, \tag{1.35}$$

де

$$R_m = \sum_{r=1}^{m-1}\sum_{i_1,\dots i_{m-r}} \Theta_m^{(r)} l_{i_1} \dots l_{i_{m-r}} E_m^{(r)} p^{(r-m-1)n} \log^r n,\ \left|\Theta_m^{(r)}\right| < 1 \tag{1.36}$$

Дійсно, якщо в (1.33) всі координати t дорівнюють нулю, то маємо внесок $l_1 \dots l_m p^n N_m$.

Нехай r координат вектора t відмінні від нуля, для зручності нехай це

будуть $t_1, \dots, t_r$. Сумуючи в (1.33) по ξ отримуємо

$$l_{r+1} \dots l_m \sum_u \sum_{(x)} \sum_{(t)}{}^* e^{2\pi i(uf(x)+t\cdot(x-\xi))/p^n} \frac{1-e^{-2\pi i(l_1 t_1/p^n)}}{1-e^{-2\pi i(t_1/p^n)}} \dots \frac{1-e^{-2\pi i(l_r t_r/p^n)}}{1-e^{-2\pi i(t_r/p^n)}}, \tag{1.37}$$

$*$ - означає, що сумуємо лише по $t_1, \dots, t_r$.

(1.37) за модулем не перевищує

$$l_{r+1} \dots l_m \sum_{(t)}{}^* E_m^{(r)} (\sin \frac{\pi t_1}{p^n} \dots \sin \frac{\pi t_r}{p^n})^{-1} < l_{r+1} \dots l_m E_m^{(r)} p^{2n} \log^r p^n.$$

Проводячи сумування по r та враховуючи комбінації наборів індексів з r, отримуємо відношення (1.35) і (1.36).

Зауважимо, що якщо деякі з l_i кратні p^{n-1}, то у виразі (1.37) можемо вважати, що при сумуванні по відповідному t_i, він набуває значення, взаємно прості з p, а отже в (1.34) оцінку ведемо по всім значенням t_i.

Застосуємо отримані результати до задачі про розподіл розв'язків конгруенції

$$ax^3 + y^3 \equiv b \ (mod\ p^n),\ (a,p) = (b,p) = 1,\ p = 6k-1, \tag{1.38}$$

де $0 \le x < T_1$, $0 \le y < T_2$.

Як було показано в [2] дана задача еквівалентна задачі про розподіл сукупності розв'язків конгруенцій виду

$$y \equiv y(0)\phi(t)(mod\ p^n), \tag{1.39}$$

де $0 \le y < T_2$, $0 \le t < \left[\frac{T_1}{p}\right] = Q$. Тут $y(0)$ - розв'язок (1.38), а x приймає значення 0, 1, $\dots$, $p-1$, виключаючи випадок, коли $ax_0^3 \equiv b(mod\ p)$.

Для зручності викладок замінимо t на x в (1.39) і тоді маємо

$$f(x,y) = y(0)\phi(x) - y, \tag{1.40}$$

де $\phi(x) = a_0 + a_1 p^{\lambda_1} x + \ldots + a_s p^{\lambda_s} x_s$, $(a_i,p) = 1$.

Розглядаємо наступну задачу

$$f(x,y) \equiv 0 \ (mod\ p^n), 0 \le x < Q, 0 \le y < T_2, (y,p) = 1. \tag{1.41}$$

Будемо вважати, що $T_2 = kp^{n-1}$, $0 < k \le p$.

Використовуючи формули (1.35) та (1.36) маємо

$$N'_{Q,\ T_2} = \frac{QT_2}{p^{2n}} N + \Theta E_2^{(2)} p^{-n} \log^2 p^n + R_2,\ |\Theta| \le 1, \tag{1.42}$$

де

$$R_2 = \Theta' E_2^{(1)} (Q + T_2) p^{-2n} \log p^n,\ |\Theta'| \le 1. \tag{1.43}$$

$N'_{q,\ T_2}$ - кількість розв'язків конгруенції (1.41), а N- кількість розв'язків конгруенції

$$y \equiv y(0)(a_0 + a_1 p^{\lambda_1} x + \ldots + a_s p^{\lambda_s} x^s) \ (mod\ p^n),\ (y,p) = 1. \tag{1.44}$$

Було доведено, що при $i > 4$ справедлива нерівність $\lambda_i \ge i\dfrac{p-2}{p-1} > 0$, а отже многочлен $\phi(x)$ за модулем p є многочленом 3-го степеня і тоді конгруенція $\phi(x) \equiv 0 \ (mod\ p)$ має не більше трьох розв'язків.

Звідки отримуємо, що при $x = 0, 1, \ldots, p^n - 1$ многочлен $\phi(x)$ набуває кратних p значень не більше ніж $3p^{n-1}$.

Конгруенція (1.41) має рівно p^n розв'язків, оскільки при кожному значенні x величина y визначається однозначно і не більше ніж $3p^{n-1}$ раз y

буде кратним p. Таким чином маємо

$$N = p^n + O(p^{n-1}).$$

Щоб отримати оцінки для $E_2^{(1)}$ і $E_2^{(2)}$ використаємо теорему, сформульовану в довіднику Хуа Ло-Гена [4].

Теорема 1. *Нехай* $f(x) = a_1x + \ldots + a_kx^k$ *- многочлен з цілими коефіцієнтами і нехай* m*- найбільше ціле таке, що* $(a_m,p) = 1$*. Тоді, якщо* $1 \leq m < p$*, то справедлива наступна оцінка*

$$\left| \sum_{x=1}^{p^n} e^{2\pi i(f(x)/p^n)} \right| \leq m^n p^{n(1-1/m)} \tag{1.45}$$

Маємо

$$E_2^{(r)} = \sum_{u=o}^{p^n-1} \sum_{x,y=0}^{p^n} e^{2\pi i(u(y(0)\phi(x)-y)/p^n+(t_1x+t_2y)/p^n)} =$$
$$= \sum_u \sum_y e^{2\pi i((t_2-u)/p^n)y} \sum_x e^{2\pi i(uy(0)\phi(x)+t_1x)/p^n}$$

Звідки

$$\left|E_2^{(r)}\right| \leq \sum_u \left| \sum_y e^{2\pi i((t_2-u)/p^n)y} \right| \left| \sum_x e^{2\pi i(uy(0)\phi(x)+t_1x)/p^n} \right|$$

Сума $\sum_y e^{2\pi i((t_2-u)/p^n)y}$ дорівнює нулю, крім випадку $u = t_2$, тоді вона дорівнює p^n.

Зауважимо, що сумування по u вдеться тільки при $(u,p) = 1$.

У цьому випадку до суми $e^{2\pi i(uy(0)\phi(x)+t_1x)/p^n}$ може бути застосована Теорема (1), причому $m \leq 3$.

В результаті отримаємо

$$\left|E_2^{(r)}\right| \leq p^n 3^n p^{2/3n} = 3^n p^{5/3n},\ r = 1{,}2.$$

Отримуємо наступну рівність

$$N'_{Q,T_2} = \frac{T_2 Q}{p^n} + O\left(\frac{T_2 Q}{p^{n+1}}\right) + 3^n p^{2/3n} \log^2 p^n + 3^n (Q + T_2) p^{-1/3n} \log p^n \quad (1.46)$$

Нехай тепер $kp^{n-1} < T_2 < (k+1)p^{n-1}$, звідки $N'_{Q,kp^{n-1}} \leq N'_{Q,T_2} \leq N'_{Q,(k+1)p^{n+1}}$.

Завдяки цьому отримуємо

$$N'_{Q,T_2} = \frac{T_2 Q}{p^n} + O\left(\frac{T_2 Q}{p^n k}\right) + 3^n p^{2/3n} \log^2 p^n + 3^n (Q + T_2) p^{-1/3n} \log p^n$$

Або, якщо записати інакше

$$N'_{Q,T_2} = \frac{T_2 Q}{p^n} + O\left(\frac{T_2 Q}{p^n k}\frac{1}{k}\right) + O\left(e^{2n} p^{2/3n} \log^2 p\right) \quad (1.47)$$

Позначимо через $A(T_1,\, T_2)$ кількість розв'язків конгруенції (1.38), та беручі до уваги рівномірність оцінки (1.47) відносно x, отримаємо, що для кількості розв'язків справедлива наступна асимптотична формула

$$A(T_1,\, T_2) = \frac{T_1 T_2 p - 1}{p^n}\frac{}{p} + O\left(\frac{T_1}{p}\right) + O\left(e^{2n} p^{2/3n} \log^2 p\right) \quad (1.48)$$

РОЗДІЛ 2

ОЦІНКА КІЛЬКОСТІ РОЗВ'ЯЗКІВ КОНГРЕУНЦІЙ

Метод Л.П. Постнікової (1964) [2] дозволяє дослідити розподіл розв'язків широкого класу конгруенцій вищих ступенів.

2.1 Оцінка кількості точок з цілими координатами на еліптичних кривих

Розглянемо конгруенцію

$$y^2 \equiv x^3 + a(mod\ p^n), \tag{2.1}$$

де $a \not\equiv 0(mod\ p)$, p – просте, $n \in \mathbb{N}$

Нехай x_0 - розв'язок (2.1), тоді $x_0 + pt$ також буде розв'язком. Тоді (2.1) набуде наступного виду

$$y^2 \equiv (x_0 + pt)^3 + a(mod\ p^n).$$

Отже будемо мати

$$y^2 \equiv (x_0^3 + a)(1 + 3x_0'x_0^2pt + 3x_0'x_0(pt)^2 + x_0(pt)^3)(mod\ p^n),$$

де $(x_0^3 + a)x_0' \equiv 1(mod\ p^n)$ і $1 \leq x_0' \leq p^n - 1$.

Розглядаючи x_0, x_0' і ω як дійсні числа, введемо у розгляд функцію

$$U(\omega) = \sqrt{1 + 3x_0'x_0^2\omega + 3x_0'x_0\omega^2 + x_0\omega^3}$$

.

Розкладемо функцію $U(\omega)$ в степеневий ряд

$$U(\omega) = \sum_{l=0}^{\infty} X_l\omega^l,$$

де $X_l = X_l(x_0, x_0')$ функції від x_0, x_0'. Зрозуміло, що $X_0 = 1$, $X_1 = 3/2x_0^2x_0'$. Розглянемо похідну $\ln U(\omega)$

$$\frac{d(\ln U(\omega))}{d\omega} = \frac{U'(\omega)}{U(\omega)} = \frac{\sum_{l=1}^{\infty} lX_l\omega^{l-1}}{\sum_{l=0}^{\infty} X_l\omega^l}. \tag{2.2}$$

З іншого боку

$$\frac{d(\ln U(\omega))}{d\omega} = \frac{3x_0^2x_0' + 6x_0x_0'\omega + 3x_0'\omega^2}{2 + 6x_0^2x_0'\omega + 6x_0x_0'\omega^2 + 2x_0'\omega^3} \tag{2.3}$$

Прирівнюючи (2.2) і (2.3) отримуємо

$$\sum_{l=1}^{\infty} lX_l\omega^{l-1}(2+6x_0^2x_0'\omega+6x_0x_0'\omega^2+2x_0'\omega^3)-\sum_{l=0}^{\infty} X_l\omega^l(3x_0^2x_0'+6x_0x_0'\omega+3x_0'\omega^2) = 0$$

Звідки при $k = 1, 2, \ldots$

$$2X_{k+1} = (3 - 6k)x_0^2x_0'X_k + (12 - 6k)x_0x_0'X_{k-1} + (7 - 2k)x_0'X_{k-2} \tag{2.4}$$

З формули (2.4) можемо отримати всі X_{k+1}, при

$$X_0 = 1,\ X_1 = \frac{3}{2}x_0^2x_0',\ X_2 = -\frac{9}{4}x_0^4(x_0')^2 + 3x_0x_0'.$$

Аналогічно для

$$y^2 \equiv x^3 + ax + b(mod\ p^n), \tag{2.5}$$

де $a,\ b \not\equiv 0(mod\ p)$, отримуємо функцію

$$U(\omega) = \sqrt{1 + (3x_0^2 + a)x_0'\omega + 3x_0x_0'\omega^2 + x_0'\omega^3}, (x_0^3 + ax_0 + b)x_0' \equiv 1(mod\ p^n)$$

Для якої справедлива наступна рівність

$$\frac{d(\ln U(\omega))}{d\omega} = \frac{(3x_0^2 + a)x_0' + 6x_0x_0'\omega + 3x_0'\omega^2}{2 + 2x_0'(3x_0^2 + a)\omega + 6x_0x_0'\omega^2 + 2x_0'\omega^3} \tag{2.6}$$

Звідки при $k = 1, 2, \ldots$

$$(2k+2)X_{k+1} = (3x_0^2+a)(1-2k)x_0'X_k+6(2-k)x_0x_0'X_{k-1}+(7-2k)X_{k-2} \tag{2.7}$$

З формули (2.7) можемо отримати всі X_{k+1}, при

$$X_0 = 1,\ X_1 = \frac{1}{2}(3x_0^2 + a)x_0',$$
$$X_2 = \frac{3}{2}x_0x_0' - \frac{1}{8}(3x_0^2 + a)^2x_0x_0',$$

де $(x_0^3 + ax_0 + b)x_0' \equiv 1(mod\ p^n)$.

Що в свою чергу доводить твердження леми, аналогічної лемі 3 в роботі [2]:

Лема 1. *Нехай* $s = \left[\frac{p-1}{p-2}n\right]$, $y_1(t)$, $y_2(t)$ — *розв'язки* (2.5). *Існує многочлен степені* s

$$\phi(t) = \Phi_0(x_0) + p^{\lambda_1}\Phi_1(x_0)t + \ldots + p^{\lambda_s}\Phi_s(x_0)t^s,$$

у якого $\Phi_i(x_0)$, $i = 0,\ 1,\ \ldots,\ s$ *— натуральні числа, які взаємно прості з* p, *а* $\lambda_1,\ \lambda_2,\ \ldots,\ \lambda_s$ *— натуральні числа, для яких справедливі нерівності*

$$\lambda_j \geq j\frac{p-2}{p-1},\ j = 1,\ \ldots,\ s,$$

такий, що розв'язки конгруенції (2.5)

$$y_i(t) \equiv y_i(0)\phi(t)\ (mod\ p^n),\ i = 1,\ 2$$

Далі введемо у розгляд величини Y_j, Z_j $(j = 1,\ 2,\ \ldots,\ s)$, які визначаються наступним чином

$$Y_1 = 0,\ Y_2 = 1,\ Y_3 = \frac{1}{2}x_0'(3x_0^2 + a)$$
$$Z_1 = 0,\ Z_2 = 0,\ Z_3 = 1,$$

а при $j \geq 4$, Y_j, Z_j знаходимо з формули (2.7), замінюючи X на відповідні змінні.

Розглянемо визначники

$$\Delta_j = \begin{vmatrix} X_{j-2} & X_{j-1} & X_j \\ Y_{j-2} & Y_{j-1} & Y_j \\ Z_{j-2} & Z_{j-1} & Z_j \end{vmatrix},\ j = 3,\ 4,\ \ldots,\ s.$$

Враховуючи введені позначення для Δ_3 будемо мати

$$\Delta_3 = \begin{vmatrix} X_1 & X_2 & X_3 \\ Y_1 & Y_2 & Y_3 \\ Z_1 & Z_2 & Z_3 \end{vmatrix} = X_1 \begin{vmatrix} Y_2 & Y_3 \\ Z_2 & Z_3 \end{vmatrix} = \frac{1}{2}(3x_0^2 + a)x_0'.$$

Отримуємо, що $\nu_p(\Delta_3) = 0$, тобто $(\Delta_3,\ p) = 1$.

Крім того для $j \geq 4$ отримуємо:

$$\Delta_j = \begin{vmatrix} X_{j-2} & X_{j-1} & X_j \\ Y_{j-2} & Y_{j-1} & Y_j \\ Z_{j-2} & Z_{j-1} & Z_j \end{vmatrix} = -\frac{2j-9}{2j} \begin{vmatrix} X_{j-2} & X_{j-1} & X_{j-3} \\ Y_{j-2} & Y_{j-1} & Y_{j-3} \\ Z_{j-2} & Z_{j-1} & Z_{j-3} \end{vmatrix} = -\frac{2j-9}{2j}\Delta_{j-1}$$

Повторюючи дані міркування можна отримати, що

$$\Delta_j = (-x_0')^{j-3}\frac{(2j-9)!6}{2^{2j-7}j!(j-4)!}\Delta_3$$

Далі нехай

$$\nu_p(X_j p^j) = \lambda_j,\ \nu_p(Y_j p^j) = \mu_j,\ \nu_p(Z_j p^j) = \tau_j$$

і тоді остаточно, враховуючи вираз для Δ_j, отримуємо, що

$$\min\left(\lambda_{j-2},\lambda_{j-1},\lambda_j\right) \leq j + 1 + \frac{4(j-1)}{p-1}$$

Використовуючи всі попередні результати було отримано наступні результати для конгруенції (2.5)

Теорема 2. *Нехай $p > 3$ — просте число, $n \in \mathbb{N}$, $n \geq 3$, $A(T_1, T_2)$ — кількість розв'язків (2.5). Де $0 \leq x \leq T_1$, $0 < y \leq T_2$,*

$$p^{\frac{5n+23}{8}} \leq T_1 \leq p^n,\ 1 \leq T_2 \leq p^n.$$

Тоді

$$A(T_1, T_2) = \frac{T_1 T_2}{p^n} + O(e^{7n\log^2 n}T_1^{\theta}),\ \theta = 1 - \frac{1}{32n^3\log n}.$$

2.2 Розподіл розв'язків

$$y^2 \equiv x^4 + x^2 + a \ (mod \ p^n)$$

Розглянемо конгруенцію

$$y^2 \equiv x^4 + x^2 + a(mod\ p^n), \tag{2.8}$$

де $a \not\equiv 0(mod\ p)$, p - просте, $n \in \mathbb{N}$.

Допоміжна функція $U(\omega)$ для конгруенції (2.7):

$$U(\omega) = \sqrt{1 + x_0'(4x_0^3 + 2x_0)\omega + x_0'(6x_0^2 + 1)\omega^2 + 4x_0'x_0\omega^3 + x_0'\omega^4},$$

де $(x_0^4 + x_0^2 + a)x_0' \equiv 1(mod\ p^n)$.

Для якої справедлива наступна рівність:

$$\frac{d(\ln U(\omega))}{d\omega} = \frac{x_0'(4x_0^3 + 2x_0) + 2x_0'(6x_0^2 + 1)\omega + 12x_0x_0'\omega^2 + 4x_0'\omega^3}{2 + 2x_0'(4x_0^3 + 2x_0)\omega + 2x_0'(6x_0^2 + 1)\omega^2 + 8x_0'x_0\omega^3 + 2x_0'\omega^4} \tag{2.9}$$

Звідки при $k = 1, 2, \ldots$

$$(k+1)X_{k+1} = X_k x_0'(2x_0^3 + x_0)(1 - 2k) + X_{k-1}x_0'(6x_0^2 + 1)(3 - k) + \\ + 2X_{k-2}x_0x_0'(7 - 2k) + \frac{1}{2}X_{k-3}x_0'. \tag{2.10}$$

З формули (2.10) отримуємо всі X_{k+1} при

$$X_0 = 1,\ X_1 = -x_0'(2x_0^3 + x_0)$$

$$X_2 = \frac{(x_0')^2}{2}(2x_0^3 + x_0)^2 + \frac{x_0'}{2}(6x_0^2 + 1),$$

$$X_3 = -\frac{(x_0')^3}{2}(2x_0^3 + x_0)^3 - \frac{(x_0')^2}{2}(6x_0^2 + 1)(2x_0^3 + x_0) + \frac{x_0'}{6}$$

Далі, аналогічно результатам попереднього розділу, можна отримати оцінки для λ_j, ввести у розгляд величини Δ_i і отримати вирази для розв'язків конгруенції (2.8).

2.3 Розподіл розв'язків $x^s + y^m \equiv 1(mod\ p^n)$

Розглянемо конгруенцію загального виду

$$x^s + y^m \equiv 1(mod\ p^n), \tag{2.11}$$

де s, m, $n \in \mathbb{N}$, p – просте.

Введена у розгляд функція $U(\omega)$, згідно методу, який запропонувала Л.П. Постнікова (1964) [2], для конгруенції (2.10) набуде наступного вигляду

$$U(\omega) = \sqrt[m]{1 - sx_0^{s-1}x_0'\omega - C_s^2 x_0^{s-2}x_0'\omega^2 - \ldots - C_s^{s-1}x_0x_0'\omega^{s-1} - x_0'\omega^s}, \tag{2.12}$$

де C_s^k – біноміальні коефіцієнти і $(1 - x_0^s)x_0' \equiv 1(mod\ p^n)$. Звідки отримуємо вираз для знаходження X_l:

$$\sum_{l=1}^{\infty} lX_l\omega^{l-1}(m - C_s^1 mx_0'x_0^{s-1}\omega - \ldots - C_s^{s-1}x_0'x_0\omega^{s-1} - x_0'm\omega^s) + \\ + \sum_{l=0}^{\infty} X_l\omega^l(C_s^1 mx_0'x_0^{s-1} + 2C_s^2 x_0'x_0^{s-2}\omega + \ldots + C_s^{s-1}x_0'x_0(s-1)\omega^{s-2} + x_0's\omega^{s-1}) = 0 \tag{2.13}$$

Звідки при $l = 1, 2, \ldots s$, використовуючи наведену нижче таблицю (Табл.2.1) отримуємо всі X_l.

Для всіх $l = s+1,\ s+2, \ldots$ отримуємо наступну рекурентну формулу:

$$(l+1)X_{l+1}m = -X_l l x_0' x_0^{l-1}(1 - lm) - X_{l-1}C_s^2 x_0' x_0^{l-2}(2 - (l-1)m) - \ldots \\ - X_2 C_s^{s-1}x_0'x_0(l - 1 - 2m) - X_1 x_0'(l - m). \tag{2.14}$$

$l=0$	0	$X_0C_s^1x_0'x_0^{s-1}$	$2X_0C_s^2x_0'x_0^{s-2}$	$\vdots$	$X_0C_s^{s-1}x_0'x_0\times$ $\times(s-1)$	sX_0x_0'
$l=1,\ \omega^0$	mX_1	$X_1C_s^1x_0'x_0^{s-1}\times$ $\times(1-m)$	$X_1C_s^2x_0'x_0^{s-2}\times$ $\times(2-m)$	$\vdots$	$X_1C_s^{s-1}x_0'x_0\times$ $\times(s-1-m)$	$X_1x_0'(s-m)$
$l=2,\ \omega$	$2mX_2$	$X_2C_s^1x_0'x_0^{s-1}\times$ $\times(1-2m)$	$X_2C_s^2x_0'x_0^{s-2}\times$ $\times(2-2m)$	$\vdots$	$X_2C_s^{s-1}x_0'x_0\times$ $\times(s-1-2m)$	$X_2x_0'(s-2m)$
$l=3,\ \omega^2$	$3mX_3$	$X_3C_s^1x_0'x_0^{s-1}\times$ $\times(1-3m)$	$X_3C_s^2x_0'x_0^{s-2}\times$ $\times(2-3m)$	$\vdots$	$X_3C_s^{s-1}x_0'x_0\times$ $\times(s-1-3m)$	$X_3x_0'(s-3m)$
$l=4,\ \omega^3$	$4mX_4$	$X_4C_s^1x_0'x_0^{s-1}\times$ $\times(1-4m)$	$X_4C_s^2x_0'x_0^{s-2}\times$ $\times(2-4m)$	$\vdots$	$X_4C_s^{s-1}x_0'x_0\times$ $\times(s-1-4m)$	$X_4x_0'(s-4m)$
$\dots$	$\dots$	$\dots$	$\dots$	$\ddots$	$\dots$	$\dots$
$l=s-1,\ \omega^{s-2}$	$(s-1)mX_{s-1}$	$X_{s-1}C_s^1x_0'x_0^{s-1}\times$ $\times(1-(s-1)m)$	$X_{s-1}C_s^2x_0'x_0^{s-2}\times$ $\times(2-(s-1)m)$	$\vdots$	$X_{s-1}C_s^{s-1}x_0'x_0\times$ $\times(s-1-(s-1)m)$	$X_{s-1}x_0'(s-(s-1)m)$
$l=s,\ \omega^{s-1}$	smX_s	$X_sC_s^1x_0'x_0^{s-1}\times$ $\times(1-sm)$	$X_sC_s^2x_0'x_0^{s-2}\times$ $\times(2-sm)$	$\vdots$	$X_sC_s^{s-1}x_0'x_0\times$ $\times(s-1-sm)$	$X_sx_0'(s-sm)$
$l=s+1,\ \omega^s$	$(s+1)mX_{s+1}$	$X_{s+1}C_s^1x_0'x_0^{s-1}\times$ $\times(1-(s+1)m)$	$X_{s+1}C_s^2x_0'x_0^{s-2}\times$ $\times(2-(s+1)m)$	$\vdots$	$X_{s+1}C_s^{s-1}x_0'x_0\times$ $\times(s-1-(s+1)m)$	$X_{s+1}x_0'(s-(s+1)m)$

Табл. 2.1: Коефіцієнти в (2.9) при відповідних степенях ω.

2.4 Застосування отриманих результатів для дослідження кількості розв'язків

Отримані уявлення ровз'язків розглянутих вище конгруенцій дозволяє розв'язати задачу про кількість розв'язків виду $(x(t), y(t))$, $t = 0, 1, \ldots, T-1$, які попали у прямокутник

$$1 \leq x \leq T_1,\ 1 \leq y \leq T_2,$$

тобто задачу про розподіл розв'язків конгруенцій виду

$$y^k \equiv f(x)\ (mod\ p^n)$$

де $f(x)$ — многочлен типу $x^l \not\equiv bx + c$, в неповних системах лишків $1 \leq x \leq T_1$, $1 \leq y \leq T_2$, T_1, $T_2 \leq p^n$.

Дійсно, шукана кількість розв'язків дорівнює сумі значень характеристичної функції $\chi(\Delta)$, де Δ — інтервал $\left[\frac{1}{p^n}, \frac{T_2}{p^n}\right]$. Ця сума оцінюється за домогою леми про скляночки Виноградова за допомогою оцінок тригонометричної суми

$$\sum_{i=1}^{k} \sum_{x_0} \sum_{t=1}^{T} e^{2\pi i \frac{\phi_i(0)\phi(t)}{p^n}}$$

тут $\phi(t) = \Phi_0(x_0) + p^{\lambda_1}\Phi_1(x_0) + \ldots$.

Внутрішню суму по t можна оцінювати двома способами:

1. Теорема Виноградова про середнє значення тригонометричної суми (див. [5]) по коефіцієнту многочлена $\phi(t)$ з номером $(s-1)$ або s, де s — степінь многочлена $\phi(t)$ призводить до оцінки суми по t як $<< T^{1-\rho}$, де $\rho = 1 - \dfrac{c_0}{n^2 \log n}$, c_0— абсолютна постійна, яка залежить тільки від вигляду $\phi(t)$, а тоді асимптотична формула в задачі про кількість

розв'язків конгруенції набуває вигляду

$$A(T_1,\, T_2) = \frac{T_1 T - 2}{p^n} + O\left(T_2^{1-\rho}\frac{T_1}{p^n}\right)$$

2. Обчислення коефіцієнтів при t в многочлені $\phi(t)$ показує, що для $p > 7$ многочлен $\phi(t)$ набуває вигляду $\phi(t) = A_0 + A_1 t + A_2 t^2 + p^3 g(t)$, де $g(x) \in \mathbb{Z}\,[t]$. Але тоді сума

$$\sum_t e^{2\pi i y_i(0)(A_0 + A_1 t + A_2 t^2 + p^3 g(t))},$$

де $g(t)$ — многочлен з цілими коефіцієнтами,$\nu_p(A_2) = 2$. Тому сума по t є неповною сумою Гауса, яку можна оцінити через повну суму Гауса (яка в свою чергу оцінюється як квадратний корінь з довжини суми, тобто $<< p^{n/2}$)

Ці два способи оцінок суми

$$\sum_t exp\left\{2\pi i y_i(0)\frac{\phi(t)}{p^n}\right\}$$

призводять до оцінки остаточного члена в асимптотичній формулі для $A(T_1,\, T_2)$.

$$A(T_1,\, T_2) = \frac{T_1 T_2}{p^n} + O\left(\min\left\{\frac{T_1}{p^n}(T_1^{1-\frac{c_0}{n^2\log n}}),\, \frac{T_2}{p^{n/2}\log p^n}\right\}\right)$$

Враховуючи отримані результати можемо сформулювати наступну теорему

Теорема 3. *В позначеннях теореми 2 отримуємо*

$$A(T_1,T_2) = \frac{T_1 T_2}{p^n} + O(p^{\frac{n}{2}}\log^2 p^n).$$

ВИСНОВКИ

У даній роботі було проведено глибоке дослідження ряду конгруенцій з використаням методу тригонометричних сум з метою отримання асимптотичних формул для кількості їхніх розв'язків.

Результати роботи показали, якого виду тригонометричні суми виникають при оцінці кількості розв'язків конгруенцій, та якими методами їх можна оцінити.

Важливим етапом дослідження було визначення двох ефективних методів оцінки цих сум: перший базується на використанні теореми Виноградова про середне значення тригонометричної суми, а другий включає обчислення коефіцієнтів при t у многочлені $\phi(t)$, який виникає при побудові уявлень розв'язків конгруенцій.

Здобуті результати в рамках даної роботи мають важливе теоретичне значення та практичний потенціал у галузі теорії чисел та аналітичної теорії чисел. Вони можуть бути використані для подальшого розвитку аналітичних та обчислювальних методів у аналітичній теорії чисел, а також знайти застосування у суміжних областях, таких як криптографія і обробка сигналів.

СПИСОК ЛІТЕРАТУРИ

[1] **Louis Joel Mordell** Incomplete exponential sums and incomplete residue systems for congruences, Czechoslovak Mathematical Journal, Vol. 14 (1964), No. 2, 235–242

[2] **Л.П. Постнікова** Розподіл розв'язків конгруенції $x^2+y^2 \equiv 1(mod\, p^n)$, Матем. сб., 1964, том 107, №2, 228-238

[3] **J. Wright** On polynomial congruence, The University of Edinburgh, 2017, pp 1-15

[4] **Ло-Ген Хуа** Метод тригонометричних сум та його застосування в теорії чисел, Видавництво "Мир" , 1964, 187

[5] **Виноградов І. М.** Метод тригонометричних сум в теорії чисел – 2 вид. – М.,1976.

[6] **Klishyn M., Varbanets P.** The distribution of points of the elliptic curve over the finite ring // XIV Ukraine Algebra Conference. – 2023. – 75 с.