Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ”

Кафедра математики факультету інформатики

Курсова робота на тему:
Кола на решітках

Керівник курсової роботи:
канд. фіз.-мат. наук,
старший викладач
Тимошкевич Л. М.
(прізвище та ініціали)

_____
(підпис)
“____”_____ 2021 р.

Виконав студент
3-го року навчання спеціальності
113 “Прикладна математика”
Осадчий Антон Олександрович
(ПІБ)

Київ – 2021

Зміст

1 Вступ

Математика – величезний набір задач та теорій, створених для їх розв'язання. Хоча задач існує безліч, зовсім не всі вони мають щось особливе в собі, щось, що віками захоплює розуми математиків від дорослих до малих. Задача, про яку йдетиметься в цій роботі, є саме такою. Першим дослідженням кіл на решітках зайнявся відомий як "Король Математиків"Карл Фрідріх Гаус, який продемонстрував, що насправді ця задача пов'язана з іншою цікавою областю математики, а саме представленням чисел як суми двох квадратів.

К. Гаус революціонував останню задачу цитатою "природне джерело загальної теорії варто шукати в розширенні області арифметики», він дослідив кільце цілих комплексних (Гаусових) чисел. Він показав, визначивши поняття подільності простого числа та довівши аналог основної теореми арифметики, що властивості комплексних цілих чисел нагадують добре відомі нам властивості дійсних цілих чисел. Це стало одним з найкращих прикладів використання абстрактної теорії для розв'язання конкретної арифметичної задачі. Ідеї Гауса були розвинуті роботами Карла Густава, Якоба Якобі та Фердинанда Готтхольда Ейзенштейна. А в середині XIX століття Ейзейнштейн разом з Діріхле та Шарлем Ермітом ввели та дослідили загальне поняття цілого алгебраїчного числа.

Кільце гаусових чисел стало одним з перших прикладів алгебраїчних структур з незвичайними властимостями, що стало раннім натхненням до зародження сучасної Абстрактної Алгебри, що вивчає алгебраїчні властивості, абстрагуючись від об'єктів-носіїв цих властивостей.

Сама ж задача про кола на решітках – дослідження можливих розсташуваннь кола на декартовій площині, де при заданому натуральному числі n коло містить n точок з цілочисельними координатами, або ж коли ці точки лежать безпосередньо на колі. При цьому задача про знаходження точної кількості точок, що лежать всередині круга відома як "проблема круга Гауса і є досі не розв'язаною.

Застосовують кола на решітках наприклад в криптографії, де використовуючи теорію прискорюють алгоритми знаходження точок на кривих.

2 Кола на решітках

2.1 Теореми Гауса

К. Гаус зацікавився питанням, наскільки швидко з ростом числа R зростає число $N(R)$ – кількість точок з цілими координатами що належать кругу.

$$K(R) = \{(x, y) : x^2 + y^2 \leqslant R^2\},$$

де $R \geqslant 0$ – ціле число. Число $N(R)$ дорівнює площі фігури $F(R)$, що складається з тих одиничних квадратів решітки, в яких ліній нижній кут лежить в $K(R)$ (рис. 1)

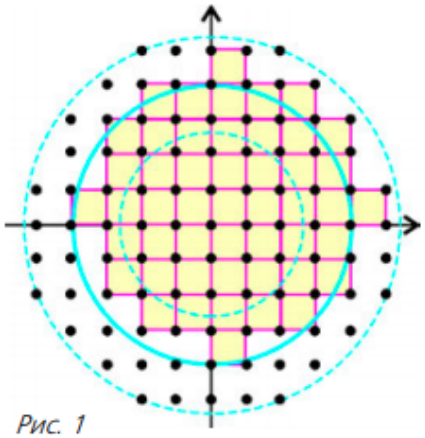


Рис. 1 [1]

Теорема 2.1. *Має місце співвідношення*

$$\lim_{R\to\infty} \frac{N(R)}{R^2} = \pi. \tag{1}$$

Доведення.

Оскільки максимальна відстань між точками двадрату зі стороною 1 не більша $\sqrt{2}$, тоді всі квадрати, що перетинаються з колом $x^2 + y^2 = R^2$ лежать на кільці (для $R = 4$ його границі зображені на рис.1)

$$\left\{(x, y) : \left(R - \sqrt{2}\right)^2 \leqslant x^2 + y^2 \leqslant \left(R + \sqrt{2}\right)^2\right\}$$

його площа дорівнює

$$\pi\left(\left(R - \sqrt{2}\right)^2 - \left(R + \sqrt{2}\right)^2\right) = 4\pi\sqrt{2}R$$

тоді

$$\left|[F(R)] - \pi R^2\right| < 4\pi\sqrt{2}R$$

де $[F(R)]$ означає площу фігури $F(R)$, отже, маємо

$$\left|\frac{N(R)}{R^2} - \pi\right| \leqslant \frac{4\pi\sqrt{2}}{R}.$$

помітимо, що для достатньо великих значеннь R має місце наближена рівність

$$\left|\frac{N(R)}{R^2}\right| \approx \pi$$

тобто

$$\lim_{R\to\infty} \frac{N(R)}{R^2} = \pi.$$

□

Гаус вручну перевірив точність формули (1), склавши таблцю значень, де можна усвідомитись, що дійсно при великих значеннях R маємо наближення до π.

R	10	20	30	100	200	300
$N(R)$	317	1257	2821	31417	125629	282697
π	3,17	3,1425	3,134	3,1417	3,140725	3,14107

[1]

Розглянемо $\mathbb{Z}^2$ породжену іншими паралелограмами. Кажуть, що паралелограм породжує решітку $\mathbb{Z}^2$, якщо вся площина розбита (без накладеннь) на рівні P паралелограми, а множина вершин всіх паралелограмів розбиття має цілочисельні координати. Такі паралелограми називаються фундаментальними.

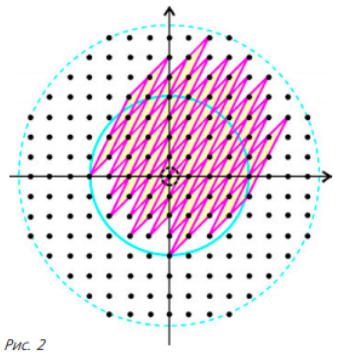


Рис. 2

[1]

Теорема 2.2. *Площа будь-якого фундаментального параллелограмма P, дорівнює 1.*

Доведення. Встановимо взаємно однозначну відповідність між фундаментальними паралелограмами та вузлами решітки $\mathbb{Z}^2$. Кожному паралелограму у відповідність поставимо його саму ліву вершину, якщо таких то, то оберему таку, у якої менша ордината. Модуль різниці площі круга та площі фігури F, що складається з паралелограмів, які відповідають вузлам із $K(R)$, менше площі кільця

$$\left\{(x,y) : (R-a)^2 \leqslant x^2+y^2 \leqslant (R+a)^2\right\},$$

де a – найбільша діагональ паралелограма P (на рис. 2 $R=4, a=\sqrt{13}$) позначимо $[P]=\Delta$, тоді $[F(R)]=\Delta N(R)$, тоді

$$\left|\Delta N(R)-\pi R^2\right| < \pi\left(((R+a)^2)-(R-a)^2\right) = 4a\pi R$$

$$\left|\frac{N(R)}{R^2}-\frac{\pi}{\Delta}\right| < \frac{4a\pi}{R\Delta}$$

Знову легко помітити, що

$$\pi = \lim_{R\to\infty}\frac{N(R)}{R^2} = \frac{\pi}{\Delta} = 1,$$

тобто $\Delta = 1$. □

Отримаємо ще один цікавий наслідок з формули (1). $N(R)$ представляє кількість всіх впорядкованих пар цілих чисел (x,y), для яких $x^2+y^2 \leqslant R^2$. Для будь-якої точки $(x,y) \in \mathbb{Z}^2$ число x^2+y^2 є цілим. Позначимо $r(k)$ як кількість всіх можливих представленнь натурального числа k як сумму двох квадратів цілих чисел (представлення $k=a^2+b^2=(-a)^2+b^2=a^2+(-b)^2=(-a)^2+(-b)^2$ вважаються попарно різними), тоді $N(R)$ можна виразити як сумму $N(R)=r(0)+r(1)+...+r(n)$, де $n=R^2$. Варто відмітити, що фунція $r(n)$ веде себе нерегулярно. Наприклад $r(0)=1, r(1)=4, r(2)=4, r(3)=0, r(4)=4, r(5)=8, r(6)=0, r(7)=0, r(8)=4$.

2.2 Гаусові числа

Перед тим як іти далі варто розглянути кільце цілих Гаусових чисел, $\mathbb{Z}[i]=\{a+bi|a,b\in\mathbb{Z}\}$, де i – умовна одиниця для якої справджується

$i^2 = -1$. Визначемо операції додавання та множення:

$$(a + bi) + (u + vi) = (a + u) + (b + v)i$$

$$(a + bi) * (u + vi) = (au - bv) + (av + bu)i$$

Означення 2.3. Спряженним до $z = a+bi$ називають число $\overline{z} = a-bi$. Основною властивістю спряженних чисел є $z\overline{z} = a^2 + b^2$.

Означення 2.4. Норма числа $z = N(z) = z\overline{z} = a^2 + b^2$.

Властивості Норми:
(1) Норма числа z дорівнює 0 лише тоді коли $z = 0$

$$N(z) = 0 \iff z = 0$$

(2) Норма числа z дорівнює нормі його спряженного

$$N(a + bi) = a^2 + b^2 = N(a - bi)$$

(3) Якщо норма числа z є непарним числом, тоді вона дає остачу 1 при діленні на 4

$$N(z) \equiv 1(\mod 2) \implies N(z) = 4n + 1, n \in \mathbb{N}$$

Доведення. Оскільки $N(z)$ – непарне число, тоді лише одне з чисел (a, b) непаре, оскільки квадрат парного числа ділиться націло на 4, а квадрат непарного має остачу 1, то сумма $a^2 + b^2 \equiv 1(\mod 4)$ □

(4) Мультиплікативність

$$N(zw) = N(z)N(w)$$

Доведення.

$$N\left((a + bi)(u + vi)\right)$$
$$= N((au - bv) + (av + bu)i) = (au - bv)^2 + (av + bu)^2 =$$
$$= (au)^2 - 2abvu + (bv)^2 + (av)^2 + 2abvu + (bu)^2 =$$
$$= (au)^2 + (bv)^2 + (av)^2 + (bu)^2 = (a^2 + b^2)(u^2 + v^2) =$$
$$= N(a + bi)N(u + vi)$$

□

З властивостей (3) та (4) слідує що дільниками одиниці є лише ті елементи, норма яких дорівнює 1, тобто $E = \{1, -1, i, -i\}$.

Означення 2.5. Асоційованими називають числа u, v
якщо $u = ev, e \in E$, тобто одне з них можливо отримати шляхом множення іншого на дільник одиниці.

Для будь-якого ненульового Гаусового числа z можна скласти множину $\{z, (-1)z, iz, (-i)z\}$. Де всі числа попарно Асоційовані, а їх норми попарно рівні. Асоційованість є відношенням еквівалентності:
1. $z = 1z$
2. $v = eu \iff N(v) = N(e)N(u) \iff N(u) = N(e)N(v) \iff u = ev$
3. $v = e_1u, u = e_2w \implies v = e_1e_2w \implies N(v) = N(e_1e_2)N(w)$
оскільки $N(v) = N(w)$, тоді $N(e_1e_2) = 1 \implies e_1e_2 \in E \implies$
$\implies v = ew, e \in E$ А отже, розбиває множину Гаусових чисел на неперетинні класси еквівалентності.

2.3 Теорія подільності Гаусових чисел

Гаусове число u ділиться(націло) на v тоді, коли існує $q \in \mathbb{Z}[i]$, таке що $u = qv$. За вл(4) норми можемо сказати, що всі гаусові числа ділятья на дільники одиниці, а отже будь-яке число, відмінне від нуля, має як мінімум 8 дільників(4 дільника одиниці, самого себе, та три асоційовані числа). Такі дільники називают тривіальними.

Означення 2.6. Простим гаусовим числом називають таке ненульове число $z \in \mathbb{Z}[i]$ що не має нетривіальних дільників.

Властивості простих гаусових чисел: (1) Якщо z – просте число, тоді $\overline{z}$ – теж просте число

$$\text{припустимо } a - bi \text{ ділиться на число } z \iff a + bi \text{ ділиться на } \overline{z}$$

(2)Норма просто гаусового числа, окрім асоційованих з $1+i$ завжди непарна, а отже, за властівістю (3) норми має вигляд $4n + 1$.

Доведення. Якщо норма числа z парна(> 2), то z ділиться на $1+i$, або асоційованого до нього числа(оскільки $r(2) = 4$, лише ці 4 чотири числа мають норму 2, а отже всі парні числа на них діляться за мультиплікативністю норми). □

Не всі прості натуральні числа є простими гаусовими, наприклад:

$$2 = (1+i)(1-i); 5 = (2+i)(2-i)$$

Означення 2.7. Взаємно простими називають такі гаусові числа u, v які не мають спільних дільників окрім дільників одиниці.

Досліджуючи кільце гаусових чисел сам Карл Фрідріх Гаус вказав критерій для простого числа $a + bi \in \mathbb{Z}[i]$. А саме, число $a + bi$ є простим тоді і тільки тоді коли
1. або одне з чисел a, b нульове, а інше є простим числом виду $4n + 3$
2. або a, b обидва не є нулями, а норма $a^2 + b^2$ є простим натуральним числом Наслідки: (1) Лише прості натуральні числа виду $4n + 3$ є простими гаусовими числами.
(2) Норма просто гаусового числа є або простим натуральним числом, або квадратом просто натурального числа.
(3) Прості натуральні числа виду $4n + 1$ можна представити як добуток двох спряжених гаусових чисел $(a + bi)(a - bi)$, цей факт в часи К.Ф. Гауса вже був відомий як Теорема Ферма–Ейлера, що стверджувала що прості числа виду $4n + 1$ можливо представити як сумму квадратів $a^2 + b^2$.
(4) Кожне просте гаусове числе є дільником одного і лише одного простого натурального числа.

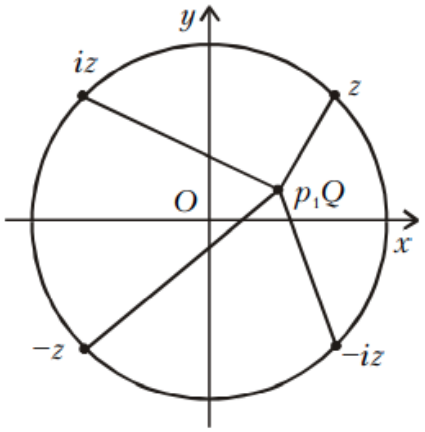
Теорема 2.8. *Розклад гаусового числа на прості множники в $\mathbb{Z}[i]$ єдиний з точністю до перестановок та асоційованості чисел*

Доведення. Припустимо, що існують гаусові числа які не мають розкладу на прості дільники, тоді розглянемо z – таке число з найменьшою нормою. Якщо z – дільник одиниці, або просте число то розклад на множники складається лише з самого числа z, інакше можемо записати z як $z = uv$, де $u, v \in \mathbb{Z}[i]$, при чому $N(u) < N(z), N(v) < N(z)$, а отже числа u та v мають розклади на прості множники, об'єднавши які можемо отримати розклад z на прості числа.
Для доведення єдиності також припустимо, що існують числа для яких існує більш ніж один унікальний розклад на прості множники, розглянемо найменьше за модулем з таких:

$$z = p_1 p_2 ... p_n = q_1 q_2 ... q_m.$$

Помітимо, що числа $p_1, p_2, ..., p_n$ попарно не асоційовані з числами $q_1, q_2, ..., q_m$, адже якщо б такі p_i та q_j існували, z/p_i за модулем менше z, але також

має більш ніж один розклад. Позначимо $P = p_2...p_n$, та $Q = q_2...q_m$. Тоді $z = p_1P = q_1Q$. Припустимо $|p_1| \leqslant |q_1|$, тоді $|Q| \leqslant |P|$, та $|p_1Q| \leqslant |z|$. Поставимо числу $w = ez - p_1Q$, де $e \in E$ – такий дільник одиниці, що $|w| < |z|$. (Обрати таке число e можливо, адже уявивши коло описане навколо квадрату породженого числами $z, -1z, iz, -iz$, точка p_1Q буде лежати всередині кола. Оскільки весь круг можливо описати кругами с центрами в вершинах квадрату з радіусом $|z|$, а точка p_1Q буде належати одному з таких кругів, можемо сказати, що існує вершина квадрату для якої відстань до p_1Q буде меньшою за $|z|$. Число w можна розкласти на множники двома



[2]

способами:

$$w = ez - p_1Q = p_1(eP - Q) = (eq_1 - p_1)q_2...q_m.$$

Оскільки $|w| < |z|$, число w має розкладатись на прості множники лиш єдиним способом. Тобто або має існувати хоча б один із множників $q_2, ..., q_m$ який кратний простому гаусовому числу p_1, що, приводить до суперечності с попарною неасоційованістю чисел $p_1, p_2, ..., p_n$, та $q_1, q_2, ..., q_m$, або число $(eq_1 - p_1)$ кратне p_1, з чого випливає, що q_1 кратне p_1 і теж є суперечністю. А одже єдиність розкладу гаусового числа на прості множники доведена. □

2.4 Представлення чисел як сумми двох квадратів

З геометричної точки зору величина $r(k)$ – кількість точок з цілочисельними координатами, що належать кругу с центром в точці початку координат.

Розглянемо формули для обчисленнь значеннь функції $r(k)$. Для натурального числа m запис $a \equiv b(\mod m)$ означає, що числа a та b маюьб однакові залишки при діленні з остачею на m, іншими словами $a = mt + b$ $(t \in \mathbb{Z})$.

Теорема 2.9. *Нехай $n > 1$ – натуральне число. Тоді*
а)

$$r(n) = 4(d_1(n) - d_3(n)),$$

де ($d_1(n)$ – кількість дільників числа n виду $4k+1$, а ($d_3(n)$ – кількість дільників числа n виду $4k+3$.
б) Якщо $n = 2^{\alpha_0} p_1^{\alpha_1} ... p_k^{\alpha_k} q_1^{\beta_1} ... q_m^{\beta_m}$ – канонічний розклад числа на прості множники, в якому $p_i \equiv 1(\mod 4), q_i \equiv 3(\mod 4)$, тоді

$$r(n) = \begin{cases} 4(\alpha_1+1)...(\alpha_k+1) & ,коли\ \beta_1, ...\beta_m\ парні \\ 0 & ,коли\ \beta_1, ...\beta_m\ непарні \end{cases}$$

Доведення. б) З теорії гаусових чисел розклад числа як сумми квадратів існує для кожного такого $v_j \in \mathbb{Z}[i]$, що $n = v_j \overline{v}_j$. Розкладемо n на прості гаусові множники $n = z_1^{a_1} z_2^{a_2} ... z_k^{a_k}$, оскільки n ділиться на v та $\overline{v}$ розклади $v = z_1^{b_1} z_2^{b_2} ... z_k^{b_k}, \overline{v} = z_1^{c_1} z_2^{c_2} ... z_k^{c_k}$ містимуть лише прості дільники числа n. За властивістю (2) норми $N(v) = N(\overline{v}) \implies$

$$\implies N(z_1^{b_1} z_2^{b_2} ... z_k^{b_k}) = N(z_1^{c_1} z_2^{c_2} ... z_k^{c_k})$$

Припустимо, існує $j < k$ таке, що $z_j = 4n+3$, при цьому $b_j \neq c_j$, що можливо тоді і тільки тоді коли z_j входить до розкладу n в непарній степені. Тоді оскільки z_j є простим числом або $N(v)$ не ділиться на $z_j^{c_j}$ коли $N(\overline{v})$ ділиться на $z_j^{c_j}$, або $N(\overline{v})$ не ділиться на $z_j^{b_j}$ коли $N(v)$ ділиться на $z_j^{b_j}$, маємо суперечність, а отже всі числа виду $4n+3$, входять до розкладу n в парній степені, або n неможливо представити як сумму двох квадратів.
Залишилось оцінити кількість пар чисел $v_j \in \mathbb{Z}[i]$, таких що $n = v_j \overline{v}_j$.
Спочатку розглянемо $n = 2^\alpha = (1+i)^\alpha (1-i)^\alpha$, існує дві пари чисел $v_1 = (1 \pm i)^{\frac{\alpha_0}{2}}, \overline{v}_1 = (1 \mp i)^{\frac{\alpha_0}{2}}$.
Схожим є випадок коли $n = q_1^{\beta_1} ... q_m^{\beta_m}$. Не існує пар $(z_j, \overline{v}_j)$, але існує єдина пара $(v_{j1} = q_1^{\beta_1/2} ... q_m^{\beta_m/2}, v_{j2} = q_1^{\beta_1/2} ... q_m^{\beta_m/2})$, що задовольяє умові $N(z_{j1}) = N(z_{j2})$, що не дає представлення n як сумми квадратів, але стане в нагоді потім.
Розглянемо випадок коли $n = p^{\alpha_1} = a^{\alpha_1} \overline{a}^{\alpha_1}$. Отже маємо умови
(1) $N(v_j) = N(\overline{v}_j)$, та
(2) $v_j \overline{v}_j = n$. З умови (2) очевидно, що розклади $v_j = a_1^m \overline{a}_1^l, \overline{v}_j = a_2^m \overline{a}_2^l$, де $m, l \in \mathbb{N}$, при чому $m_1 + l_1 = \alpha = m_2 + l_2$. А за властивостями спряжених чисел $m_1 = l_2, m_2 = l_1$. А отже всі пари чисел $(v_j, \overline{v_j})$ описуються множиною $\{((a^{\alpha-k})(\overline{a}^k), (a^k)(\overline{a}^{\alpha-k})) | 0 \leqslant k \leqslant \alpha\}$. Потужність якої $(\alpha+1)/2$.

Розглянемо випадок коли $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. З причин аналогічних до попереднього випадку маємо $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)/2$ пар $(z_j, \overline{z}_j)$ які задовільняють умовам.
Нарешті розглянемо загальний випадок коли $n = 2^{\alpha_0} p_1^{\alpha_1} ... p_k^{\alpha_k} q_1^{\beta_1} ... q_m^{\beta_m}$. Вище вже було доведено, що якщо існує непарне число β_j то представлення n як сумми квадратів не існує. Отже, щоб задовільнити умові $N(v_j) = N(\overline{v}_j)$ канонічний розклад на прості множникик v_j має містити $(1 \pm i)^{\alpha_0} q_1^{\beta_1/2} ... q_m^{\beta_m/2}$, а розклад $\overline{v}_j$ має містити $(1 \pm i)^{\alpha_0} q_1^{\beta_1/2} ... q_m^{\beta_m/2}$, а отже кількість пар $(z_j, \overline{z}_j)$ дорівнює $2(\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)$. А отже ми маємо $(\alpha_1+1)(\alpha_2+1)...(\alpha_k+1)$ пар чисел $(z_j, \overline{v}_j)$, таких що $n = z_j \overline{v}_j = a^2 + b^2$.
На останок щоб отримати вираз для $r(n)$ потрібно включити всі асоційовані с v_j, та $\overline{v}_j$ числа, тобто $r(n) = 4(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$.

□

Частковим випадком теореми 2.9 є твердження,
що рівняння $x^2 + y^2 = 5^k (k \leqslant 0)$
має $4(k + 1)$ коренів в цілих числах, іншими словами коло радіусом $5^{\frac{k}{2}}$ з центром в точці початку координат проходить в точності через $4(k + 1)$ вузлів решітки $\mathbb{Z}^2$.

За Теоремою 2.9 можливо довести, на перший погляд ніяк не пов'язану Формулу Лебніца.

Теорема 2.10. *Формула Лейбніца*

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + ... = \frac{\pi}{4}$$

Доведення.

Лема 2.11.

$$\sum_{n=1}^{R^2} d_1(n) = \left[\frac{R^2}{1}\right] + \left[\frac{R^2}{5}\right] + \left[\frac{R^2}{9}\right] + ...$$

Доведення. Розглянемо вираз $\left[\frac{R^2}{k}\right]$ $(k = 1, 5, 9, ..., 4n + 1, ...)$ дорівнює кількості чисел з множини $\{1, 2, 3, ..., R^2\}$, що діляться на k, іншими словами

$$\sum_{n=1}^{R^2} b_k(n), \text{де } b_k(n) = \begin{cases} 1, & n \equiv 0(\mod k)) \\ 0 & n \neq (\mod k) \end{cases}$$

тоді очевидно,

$$\sum_{n=1}^{R^2} b_1(n) + \sum_{n=1}^{R^2} b_5(n) + \sum_{n=1}^{R^2} b_9(n) + ... = \sum_{n=1}^{R^2} d_1(n)$$

□

Аналогічно можливо довести рівність

$$\sum_{n=1}^{R^2} d_3(n) = \left[\frac{R^2}{3}\right] + \left[\frac{R^2}{7}\right] + \left[\frac{R^2}{11}\right] + ...$$

Згідно з твердженням а) Теореми 2.9,

$$N(R) = 1 + 4\sum_{n=1}^{R^2} \left(d_1(n) - d_3(n)\right).$$

За лемою 2.11

$$\frac{1}{4}\left(N(R) - 1\right) = \left[\frac{R^2}{1}\right] - \left[\frac{R^2}{3}\right] + \left[\frac{R^2}{5}\right] - \left[\frac{R^2}{7}\right] + \left[\frac{R^2}{9}\right] - \left[\frac{R^2}{11}\right] + ...$$

$$\frac{1}{4}\left(N(R) - 1\right) = \left[\frac{R^2}{1}\right] - \left[\frac{R^2}{3}\right] + \left[\frac{R^2}{5}\right] - \left[\frac{R^2}{7}\right] + \sigma_n(R). \tag{2}$$

З одного боку $\sigma_n(R)$ невід'ємне, оскільки

$$\left(\left[\frac{R^2}{4n+5}\right] - \left[\frac{R^2}{4n+7}\right]\right) \geqslant 0$$

$$\left(\left[\frac{R^2}{4n+9}\right] - \left[\frac{R^2}{4n+11}\right]\right) \geqslant 0$$

$$\sigma_n(R) = \left(\left[\frac{R^2}{4n+5}\right] - \left[\frac{R^2}{4n+7}\right]\right) + \left(\left[\frac{R^2}{4n+9}\right] - \left[\frac{R^2}{4n+11}\right]\right) + ... \geqslant 0$$

з іншного

$$\sigma_n = \left[\frac{R^2}{4n+5}\right] - \left(\left[\frac{R^2}{4n+7}\right] - \left[\frac{R^2}{4n+9}\right]\right) - ... \leqslant \left[\frac{R^2}{4n+5}\right]$$

Нехай $R = 4n + 3$. Тоді очевидно, $0 \leqslant \sigma_n(R) \leqslant R$. Якщо в формулі (2) відкинути всі цілі частини, то її права сторона зміниться(по модулю) не біль ніж на R. Отже, маємо

$$\frac{1}{4}\left(N(R) - 1\right) = R^2\left(1 - \frac{1}{3} + ... + \frac{1}{4n+1} - \frac{1}{4n+3}\right) + 2\theta R,$$

або ж

$$\frac{N(R) - 1}{4R^2} = 1 - \frac{1}{3} + ... + \frac{1}{R-2} - \frac{1}{R} + \frac{2\theta}{R},$$

де $|\theta| \leqslant 1$. При $R \to \infty$ за теоремою 2.1 отримаємо

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + ... = \frac{\pi}{4}$$

□

2.5 Кола Шинцеля

Теорема 2.12. *Для будь-якого $n \in \mathbb{N}$ існує круг з центром в точці $(\sqrt{2}, 1/3)$, який містить в собі n точок решітки $\mathbb{Z}^2$.*

Доведення. Припустимо, що дві точки $(x_1; y_1)$ та $(x_2; y_2)$ – два різних вузла цілочисельної решітки, лежать на однаковій відстані від точки $(\sqrt{2}, 1/3)$. Тоді

$$\left(x_1 - \sqrt{2}\right)^2 + \left(y_1 - \frac{1}{3}\right)^2 = \left(x_2 - \sqrt{2}\right)^2 + \left(y_2 - \frac{1}{3}\right)^2,$$

$$\left(x_1^2 - x_2^2 + y_1^2 - y_2^2 - \frac{2}{3}y_1 + \frac{2}{3}y_2 - 2\sqrt{2}(x_1 - x_2)\right) = 0.$$

звідси випливає

$$x_1 = x_2 \text{ та } y_1^2 - y_2^2 - \frac{2}{3}y_1 + \frac{2}{3}y_2 = 0.$$

з другої рівності маємо

$$\left(y_1 - \frac{1}{3}\right)^2 = \left(y_2 - \frac{1}{3}\right)^2, \text{ або } 3y_1 - 1 = \pm(3y_2 - 1)$$

оскільки $y_1 \in \mathbb{Z}, y_2 \in \mathbb{Z}$ маємо суперечність

$$x_1 = x_2, \text{ та } y_1 = y_2$$

□

Отже, можливо обрати зростаючу послідовність радіусів R_n таку, що в колі $\left(x-\sqrt{2}\right)^2+\left(y-\frac{1}{3}\right)^2=R_n^2$ буде знаходитись рівно n точок. Біль цікавим і складним є питання про кількість точок решітки $\mathbb{Z}^2$, що можуть потрапити на коло.

Досить легко знайти кола що проходять через 1, 2, 3, 4 Приклади для $n=8$, $n=12$ та $n=6$ знайти не складно. Але для загального $n\in\mathbb{N}$ доведення не тривіальне.

Теорема 2.13. *Для будь-якого натурального числа n існує коло, що проходить рівно через n точок решітки $\mathbb{Z}^2$*

Доведення. За Теоремою 2.9, можливо побудувати коло на якому лежатиме рівно $4n$ точок. Достатньо поставити центром кола в точку начала координат, а радіусом обрати $R=5^{(n-1)/2}$ Рисунок 5 з шістьма точками на колі підсказує що варто розглянути кола с центром в точці $(\frac{1}{2};0)$. Якщо в якості радіуса взяти $R=\frac{5^{\frac{(k-1)}{2}}}{2}$, то рівняння кола запишеться як

$$\left(x-\frac{1}{2}\right)^2+y^2=\frac{5^{k-1}}{4}, \tag{3}$$

або ж

$$(2x-1)^2+(2y)^2=5^{k-1}. \tag{4}$$

За Теоремою 2.9 рівняння

$$a^2+b^2=5^{k-1} \tag{5}$$

має $4k$ коренів. В рівнянні (5) очевидно, що одне з чисел a,b має бути парним, а інше – непарним. В рівнянні (4) парність кожного доданку фіксована, отже з двох розв'язків рівняння (5) $(a,b),(b,a)$ маємо 1 розв'язок для рівняння (4) (чорні та білі точки на рисунку 6 симетричні відносно прямої $y=x-1$).Таким чином, рівняння (4) має $2k$ корені, тобто вдвічі меньше ніж рівняння (5).

Якщо ж ми хочемо обрати коло на якому непарна кількість точок решітки $\mathbb{Z}^2$ то центром не можна брати $(\frac{1}{2},0)$, адже точки симетричні прямій $x=\frac{1}{2}$. Тому розглянемо коло з центром в $(\frac{1}{3},0)$

$$\left(x-\frac{1}{3}\right)^2+y^2=\frac{5^{2k}}{9}, \tag{6}$$

$$(3x-1)^2+3y^2=5^{2k}, \tag{7}$$

Знову ж таки за Теоремою 2.9 рівняння

$$a^2 + b^2 = 5^{2k} \tag{8}$$

має $4(2k+1)$ рішеннь. Якщо розглянути остачі від ділення на 3 то можемо побачити що в рівнянні (8) одне і тільки одне з чисел (a, b) ділиться на 3(оскільки остатача при діленні на три, числа, яке є квадратом, може приймати лише 2 значення 0 або 1). Припустимо, $a \equiv 0(\mod 3), b \equiv \pm 1(\mod 3)$. Тоді з 4х пар $(a, b), (a, -b), (b, a), (-b, a)$ лише одна є розв'язком рівняння (7). А отже розв'язків рівняння (7) рівно в 4 рази маеньше ніж розв'язків (8) тобто $2k + 1$. □

Отже, ми можемо побудувати коло з будь-якою кількістю точок цілочисельної решітки які на ньому лежать.

3 Задачі

Приклад застосування Теореми 2.9:
Знайдемо $r(929500)$ за алгоритмом представленим в доведенні. Спочатку знайдемо канонічний розклад

$$929500 = 2^2 \times 5^3 \times 11 \times 13^2 = (1+i)^2(1-i)^3(2+i)^3(2-i)^3 11(3+2i)^2(3-2i)^2.$$

Тепер знайдемо всі пари $(v_j, \overline{v}_j)$:

$$v_1 = (1+i)^2(2+i)^3 11(3+2i)^2 = -1738 - 2684i$$
$$\overline{v}_1 = (1-i^2)(2-i)^3 11(3-2i)^2 = -1738 + 2684i$$

А також всі їх асоційовані числа, які приводять до представлення: $929500 = 1738^2 + 2684^2 = (-1738)^2 + 2684^2 = 1738^2 + (-2684)^2 = (-1738)^2 + (-2684)^2$.

$$v_2 = (1+i)^2(2+i)^3 11(3+2i)(3-2i) = -3146 + 572i$$

$$\overline{v}_2 = (1-i)^2(2-i)^3 11(3+2i)(3-2i) = -3146 - 572i$$

Всі представлення пов'язані з цією парою: $929500 = 3146^2 + 572^2 = (-3146)^2 + 572^2 = 3146^2 + (-572)^2 = (-3146)^2 + (-572)^2$.

$$v_3 = (1+i)^2(2+i)^3 11(3-2i)^2 = -682 + 3124i$$

$$\overline{v}_3 = (1-i)^2(2-i)^3 11(3+2i)^2 = -682 - 3124i$$

Знову бачимо: $929500 = 682^2+3124^2 = (-682)^2+3124^2 = 682^2+(-3124)^2 = (-682)^2 + (-3124)^2$.

$$v_4 = (1+i)^2(2+i)^2(2-i)11(3+2i)^2 = -3190 - 220i$$

$$\overline{v}_4 = (1+i)^2(2+i)^2(2-i)11(3+2i)^2 = -3190 + 220i$$

І за тим самим принципом можна знайти $v_5 = -1430 + 2860i$, $v_6 = 2090 + 2420i$, $v_7 = 2420 + 2090i$, $v_8 = -2860 + 1430i$, $v_9 = -2684 + 1738i$, $v_{10} = -220 - 3190i$, $v_{11} = -3124 + 682i$, $v_{12} = -572 + 3146i$. А отже маємо $r(929500) = 4(4 \times 3) = 4(12) = 48$.

Для наступних двох задач напишемо дві функції:

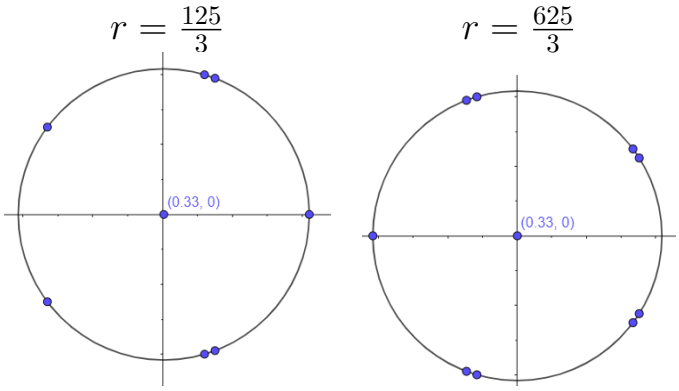
```python
#find all points with integer coordinates on a circle of radius r, with center at the point(x0, y0), with prescision eps
def findPoints(r, x0=0, y0=0, eps = 0.0001):
    points = list()
    for x in range(int(x0 - r) , int(x0 + r)+1):
        y1 = math.sqrt(r*r - ((x-x0)*(x-x0))) + y0
        yInt = round(y1)
        if abs(y1 - yInt) < eps:
            points.append((x,yInt))
        y2 = -math.sqrt(r*r - ((x-x0)*(x-x0))) + y0
        if (y2 != y1):
            yInt = round(y2)
            if abs(y2 - yInt) < eps:
                points.append((x,yInt))
    return points


def N(r):
    res = 0
    for i in range(0, r):
        for j in range(0, r):
            if i*i + j*j < r*r:
                res+=4
    return res
```

Функція $N(r)$ – кількість цілочисельних точок що лежать в колі радіуса r. Використаємо її для продовження таблиці яку вручну рахував Гаус у свій час. Маємо послідовність яка нажаль досить повільно збігається до π,

```
R =  10 N(R) =  344 N(R)/R^2 =  3.44
R =  100 N(R) =  31796 N(R)/R^2 =  3.1796
R =  1000 N(R) =  3145520 N(R)/R^2 =  3.14552
R =  10000 N(R) =  314199016 N(R)/R^2 =  3.14199016
R =  100000 N(R) =  31416325412 N(R)/R^2 =  3.1416325412
```

оскільки складність обчислення $N(R) = O(R^2)$.

Функція $findPoints()$ повертає всі точки, що лежать на колі шинцеля з центром в точці (x_0, y_0) та радіусом r. Досить цікаво подивитись на деякі приклади про які йшлося в Теоремі 2.13. Коло з центром в точкі $(\frac{1}{3}, 0)$ з радіусом у формі $r = \frac{5^k}{3}$, має лежить на $2k + 1$ вузлах решітки $\mathbb{Z}^2$.



Література

[1]Вавилов В., Устинов А. "Окружности на решетках"// Квант. – 2006. –№6

[2]Сендеров В., Співак А., "Суммы квадратов и целые гауссовы числа".

[3] Гассові целіе числа available at: http://poivs.tsput.ru/ru/Math/NumberTheory/AlgebraicNumberTheory/AlgebraicNumbers/GaussianIntegers

[4]Представление чисел суммой двух квадратов и эллиптические кривые available at: https://habr.com/ru/post/189618/