Міністерство освіти і науки України
Департамент освіти, науки та молоді Миколаївської облдержадміністрації
Миколаївське територіальне відділення Малої академії наук України

Відділення: математика
Секція: математика

Формули та асимптотичні оцінки функції R_n кількості розв'язків деяких діофантових рівнянь

Роботу виконав:
Єрмолаєв Олександр Андрійович,
учень 11 класу Миколаївського муніципального колегіуму імені Володимира Дмитровича Чайки Миколаївської міської ради

Науковий керівник:
Майборода Валерій Антонович,
старший вчитель Миколаївського муніципального колегіуму імені Володимира Дмитровича Чайки,
Миколаївської міської ради,
вчитель вищої категорії

Науковий консультант:
Воробйова Алла Іванівна,
доцент кафедри вищої математики Чорноморського державного університету імені Петра Могили,
Миколаївської міської ради,
кандидат фізико-математичних наук

Миколаїв, 2017

Миколаївське територіальне відділення МАН України

ТЕЗИ

До науково-дослідницької роботи

«Формули та асимптотичні оцінки функції R_n кількості розв'язків деяких діофантових рівнянь»

Єрмолаєва Олександра Андрійовича,

учня 11 класу Миколаївського муніципального колегіуму імені В.Д.Чайки Миколаївської міської ради

Науковий керівник – Майборода Валерій Антонович,

старший вчитель Миколаївського муніципального колегіуму імені В.Д.Чайки Миколаївської міської ради, вчитель вищої категорії

Теорія чисел у сучасному світі стає все більш актуальною. Насамперед об'єкти, задачі, ідеї, поняття та методи теорії чисел служать для створення і розвитку понять, методів, алгоритмів у різних галузях науки й техніки, наприклад. Так, багато теоретичних та практичних задач зводяться до розв'язку певних діофантових рівнянь, а встановлення їх коренів та кількості розв'язків у багатьох випадках залишається відкритою проблемою математики.

Метою даної наукової роботи є розв'язок деяких діофантових рівнянь в цілих невід'ємних числах та оцінка кількості їх розв'язків.

ЗМІСТ

Вступ

Теорія чисел займається вивченням властивостей цілих чисел, але вона займається і властивостями інших чисел: алгебраїчних, трансцендентних тощо. Теорія чисел - це також теорія алгебраїчних функцій з скінченним полем констант і аналітична теорія чисел. Якщо говорити про теперішній час, то теорія чисел на стільки розширилась, що перетворилась в безліч нових дисциплін - в сучасну алгебру, в геометрію чисел, в ймовірнісну теорію чисел і т. д.

Використовуючи традиційну термінологію ми також розрізняємо адитивну теорію чисел і аналітичну теорію чисел. Під адитивною теорією чисел розуміють розділ теорії чисел в якому вивчається можливість подання цілого числа у вигляді суми деяких наперед визначених чисел чи їх степенів. Аналітична теорія чисел - розділ теорії чисел в якому використовується апарат математичного аналізу та теорії аналітичних функцій.

Метою даної наукової роботи є розв’язок деяких діофантових рівнянь в цілих невід’ємних числах та оцінка кількості їх розв’язків.

Проблематика теорії діофантових рівнянь як правило визначається трьома типами задач:

1) дослідження можливості існування коренів на вказаній множині;
2) знаходження формул для розв’язків діофантових рівнянь;
3) оцінка кількості розв’язків діофантових рівнянь.

В даній роботі в її першій частині ми зупинимося на другому типі задач і в другому розділі ми розглянемо третій тип задач.

Розділ 1. Проблеми теорії адитивних чисел та розв'язок діофантового рівняння виду $F_n = x^2 + y^2 + z^2$, де F_n - числа Ферма

1.1. Огляд результатів по даній тематиці

Дана частина роботи може бути віднесена до області адитивної теорії чисел. Тут ми розглядаємо діофантові рівняння вигляду $a_1x_1 + a_2x_2 + \cdots + a_mx_m = n$, де всі коефіцієнти - натуральні числа та оцінюємо кількість його розв'язків у натуральних числах.

Діофантовим рівнянням називають рівняння виду $P(x_1, x_2, \ldots x_n) = a$, де $P(x_1, x_2, \ldots x_n)$ - многочлен декількох змінних із цілими коефіцієнтами, для яких потрібно знайти цілі розв'язки. Названі вони ім'ям грецького математика Діофанта Олександрійського, який жив у III столітті н. е. Його книга «Арифметика» містила в собі 189 задач із цілими числами, для кожної з яких наводилося один або декілька розв'язків.

Діофантові рівняння мають деякі специфічні ознаки, що відрізняють їх від інших рівнянь:

1) як правило, ці рівняння невизначені, тобто число рівнянь в них менше числа невідомих;
2) розв'язки повинні бути цілими числами.

Розв'язати діофантове рівняння означає:

1) з'ясувати, чи має рівняння хоча б один ненульовий розв'язок у цілих числах;

2) якщо рівняння має розв'язок в цілих числах, то з'ясувати скінченна чи нескінченна множина його розв'язків;

3) знайти всі цілі (натуральні) розв'язки рівняння.

Лінійні діофантові рівняння виду $ax + by = c$ навчились розв'язувати ще до Діофанта. Стародавні греки знали, що якщо це рівняння має один цілий розв'язок

$(x_0; y_0)$, то його буде задовольняти нескінченна множина пар $(x; y)$ виду $x = x_0 + bk; y = y_0 - bk$, де k - будь яке ціле число.

Математики Стародавньої Греції та Стародавньої Індії знали методи розв’язання деяких рівнянь другого степеня виду $ax^2 + bxy + cy^2 = dz^2$. Зокрема їм були відомі всі піфагорові трійки натуральних чисел x, y, z, що задовольняють рівняння $x^2 + y^2 = z^2$. Всі трійки взаємно простих піфагорових чисел стародавні математики знаходили за формулами $x = m^2 - n^2,\ y = 2mn,\ z = m^2 + n^2$, де m, n - натуральні числа причому $n > m$ [1].

Діофантові рівняння першої степені почали розглядатися індуськими математиками пізніше, приблизно з V століття. Деякі такі рівняння з двома і трьома невідомими з'явилися в зв'язку з проблемами, що виникли в астрономії, наприклад, при розгляді питань, пов'язаних з визначенням періодичного повторення небесних явищ.

Перший загальний розв’язок діофантового рівняння першої степені, $ax + by = c$ де a, b, c - цілі числа, зустрічається в індійського математика Брахмагупти близько 625 р.

У 1624 році публікується книга французького математика Баше де Мезірьяка, де він для вирішення рівняння застосовує процес, що зводиться до послідовного обчислення неповних приватних і розгляду відповідних дробів.

Після Баше де Мезірьяка в XVII і XVIII століттях різні правила для вирішення діофантового рівняння першої степені з двома невідомими давали Роль, Ейлер, Саундерсон та інші математики.

Ланцюгові дроби для вирішення діофантових рівнянь були застосовані Лагранжем, який, однак, зауважує, що фактично це той же спосіб, який був даний Баше де Мезірьяком і іншими математиками, які розглядали данні рівняння до нього.

У 20-х роках XX століття англійський математик Морделл висунув гіпотезу, що рівняння більш високого степеня, ніж третього, можуть мати лише скінченне число цілих розв’язків. Ця гіпотеза була в 1983 році доведена голландським математиком Фалтінгсом.

В адитивній теорії чисел вивчаються питання про представлення деякої послідовності натуральних чисел, сумою скінченного числа доданків вказаного виду.

Історично першими прикладами подібних задач стали: тернарна проблема Гольдбаха (1742 р.) про представлення непарних чисел, починаючи з 7, сумою трьох простих чисел; проблема Ейлера (1742 р.) (або бінарна проблема Гольдбаха) про представлення парних чисел, що більші за 2, у вигляді суми двох простих; проблема Варінга (1770 р.), що являється узагальненням теореми Лагранжа, яка стверджує, для кожного цілого числа $n > 1$, існує таке число $k = k(n)$, що будь-яке натуральне число N може бути представлено у вигляді $x_1^n + x_2^n + .. + x_k^n = N$, з цілими невід’ємними $x_1, x_2, \dots , x_k$; проблема Гольдбаха-Варінга, поставлена на початку 19-го століття, про представлення цілого числа сумою степенів простих чисел.

Вирішення діофантових рівнянь в натуральних - один з найкрасивіших розділів математики. Жоден великий математик не пройшов повз теорії діофантових рівнянь. Ферма, Ейлер і Лагранж, Діріхле і Гаус, Чебишев і Ріман залишили вагомий слід в цій теорії [8].

Однією з основних проблем, що не має універсального розв’язку є проблема отримання формул для довільного діофантового рівняння. В тому числі не відомо конкретної формули для знаходження кількості розв’язків таких рівняннях у загальному вигляді. У 1970 році математик Юрій Володимирович Матіясевіч довів, що загального способу, що дозволяє за скінченну кількість кроків розв’язати в цілих числах довільні діофантові рівняння, не існує і бути не може [8]. Тому для різних типів діофантового рівняння слід підбирати власні методи розв’язання. Таким чином, пошук формул та кількості розв’язків діофантових рівнянь залишається актуальною і відкритою проблемою сьогодення.

1.2. Розв'язок діофантового виду $x^2 + y^2 + z^2 = N$ $(N = F_n = 2^{2^n} + 1)$

Діофантове рівняння вигляду

$$x^2 + y^2 + z^2 = \mathrm{N} \qquad (1)$$

є частковим випадком проблеми Варінга, при *k*=3 і *n*=2.

Якщо $N = F_n = 2^{2^n} + 1$, то рівняння в цьому вигляді було запропоновано на XVII Всеукраїнському турнірі юних математиків імені професора М. Й. Ядренка (2014 рік м. Чернівці) у задачі «Зображення чисел Ферма» [4].

Сформулюємо умову задачі «Зображення чисел Ферма»:

«Числа $2^{2^n} + 1$ називаються числами Ферма. При $n \geq 3$ подайте кожне з них у вигляді суми квадратів трьох різних натуральних чисел».

В нашій роботі ми вирішили не тільки розв'язати цю задачу, але і дослідити питання більш широко, що і буде представлено далі.

Проблема Варінга-Гольдбаха ставить питання про можливість представлення цілого числа сумою степенів простих чисел. Різні варіації цієї проблеми полягають в тому, що розглядають і різні степені, і числа необов'язково прості. Ейлером було показано, що всі натуральні числа за виключенням чисел виду $4^m(8n + 7)$ *m*,*n*=0,1,2…, можна представити у вигляді суми трьох квадратів.

В даному параграфі ми розглянемо рівняння

$$F_n = x^2 + y^2 + z^2 \qquad (2),$$

де $F_n = 2^{2^n} + 1$ - числа Ферма.

Згідно з теоремою Ейлера воно має розв'язки, оскільки $F_n \neq 4^m(8n + 7)$ *m*,*n*=0,1,2… Але, по-перше, невідомі формули, що дозволяють їх знаходити, і, по-друге, невідома функція $R_3(n)$ - кількість розв'язків рівняння (1). Покажемо, як можна вирішити питання про знаходження розв'язків рівняння (2).

Теорема 1.2.1. Числа виду

$$\begin{cases} a = \dfrac{2 \times 2^{2^{n-1}} + 1}{3} \\ b = \dfrac{2^{2^{n-1}} + 2}{3} \\ c = \dfrac{2 \times 2^{2^{n-1}} - 2}{3} \end{cases} \qquad (3)$$

при $n \geq 3$ - натуральні і різні.

Доведення:

Скористаємось методом математичної індукції. Зробимо припущення, що 2 в парному степені конгурентно одиниці за модулем 3.

1. Створимо базу індукції: перевіримо справедливість твердження для $n = 1$.

$$2^2 \equiv 4(mod\ 3) \equiv 1(mod\ 3)$$

2. Зробимо припущення, що твердження правильне для $n = k$.

$$2^{2k} \equiv 1(mod\ 3)$$

3.Доведемо, що твердження правильне для $n = k + 1$.

$$2^{2(k+1)} \equiv 4(mod\ 3) \equiv 1(mod\ 3)$$

Отже, можна зробити висновок, що гіпотеза є правильною.

Оскільки $n \geq 3$, то $2^{2^{n-1}} \equiv 1(mod\ 3)$.

Звідси :

$$2^{2^{n-1}} + 2 \equiv 0(mod\ 3)$$

$$2 \times 2^{2^{n-1}} - 2 \equiv 0(mod\ 3)$$

$$2 \times 2^{2^{n-1}} + 1 \equiv 0(mod\ 3)$$

Отже, a, b і c - різні натуральні числа, що і треба було довести.

Теорема 1.2.2.

Сума квадратів чисел a, b, c, що обчислюються за формулами (3), дорівнює числам Ферма, при $n \geq 3$.

Доведення:

Дійсно, знайшовши суму квадратів вказаних чисел та застосувавши формули скороченого множення, після спрощень, отримуємо :

$$\left(\frac{2^{2^{n-1}}+2}{3}\right)^2+\left(\frac{2\times 2^{2^{n-1}}-2}{3}\right)^2+\left(\frac{2\times 2^{2^{n-1}}+1}{3}\right)^2=$$

$$=\frac{2^{2^n}+4\times 2^{2^{n-1}}+4}{9}+\frac{4\times 2^{2^n}-8\times 2^{2^{n-1}}+4}{9}+\frac{4\times 2^{2^n}+4\times 2^{2^{n-1}}+1}{9}=$$

$$=\frac{9\times 2^{2^n}+9}{9}=2^{2^n}+1=F_n$$

Теорема доведена.

Вирішити проблему знаходження однієї із серій розв'язків можна також перейшовши до двійкової системи.

Теорема 1.2.3. Всі числа Ферма $F_n = 2^{2^n}+1,\ n \geq 3$ у двійковій системі числення можуть бути подані у вигляді суми трьох квадратів (тернарної квадратичної форми) наступним чином:

$$F_n = 1\underbrace{00..00}_{2^{n-1}}1=\left(\underbrace{10..10}_{2^{n-2}-1}11\right)^2+\left(\underbrace{10..10}_{2^{n-2}}\right)^2+\left(\underbrace{10\ldots10}_{2^{n-2}-2}110\right)^2 \quad (4)$$

Правильність теореми випливає із наступних тверджень.

Лема 1.2.1. Всі числа Ферма $F_n = 2^{2^n}+1$, $n \geq 3$ у двійковій системі числення мають вигляд:

$$F_n = 1\underbrace{00..00}_{2^{n-1}}1$$

Лема 1.2.2. Для чисел виду

$$a = \underbrace{10..10}_{2^{n-2}-1}11\ , b = \underbrace{10..10}_{2^{n-2}}\ , c = \underbrace{10\ ...\ 10}_{2^{n-2}-2}110$$

справедлива рівність :

$$a^2 + b^2 + \mathrm{c}^2 = 1\underbrace{00..00}_{2^{n-1}}1$$

Справедливість леми 1 і леми 2 в свою чергу ґрунтується на теоремі про можливість запису будь-якого натурального числа в p-ічній системі числення ($p \geq 2$) єдиним способом. А також на властивостях арифметичних операцій в цих системах.

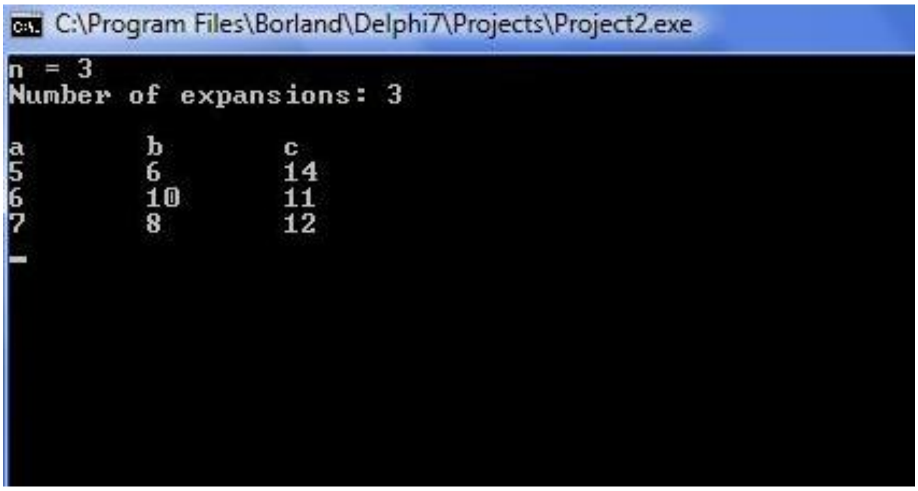
1.3. Оцінка функції $R_3(F_n)$

Під кількістю розв'язків діофантового рівняння ми, як і прийнято, розуміємо всі впорядковані набори чисел, що його задовольняють. В цьому контексті при кожному n формули (3) задають лише 6(3!) розв'язків. В той же час всі розв'язки даного рівняння не вичерпуються приведеними формулами. Шляхом створення програми «Search triples» пошуку трійок для рівняння вигляду

$$F_n = x^2 + y^2 + z^2$$

методом комп'ютерного перебору ми встановили, що для $n = 3$ існує ще дві трійки, кожна з яких задає по 6 розв'язків. Розроблена програма представлена у Додатку1. Ми представимо по одному розв'язку кожної із базових трійок.

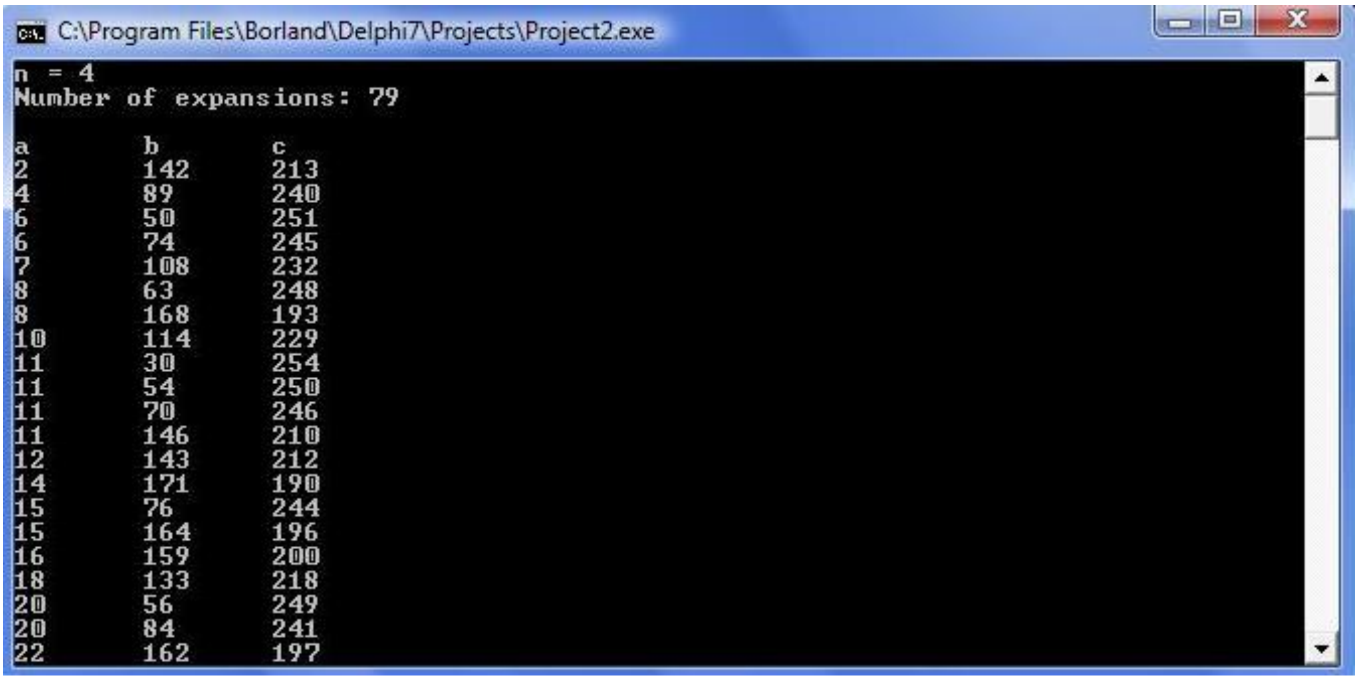
Усі можливі трійки для $n = 3$:




```
n = 3
Number of expansions: 3

a       b       c
5       6       14
6       10      11
7       8       12
```

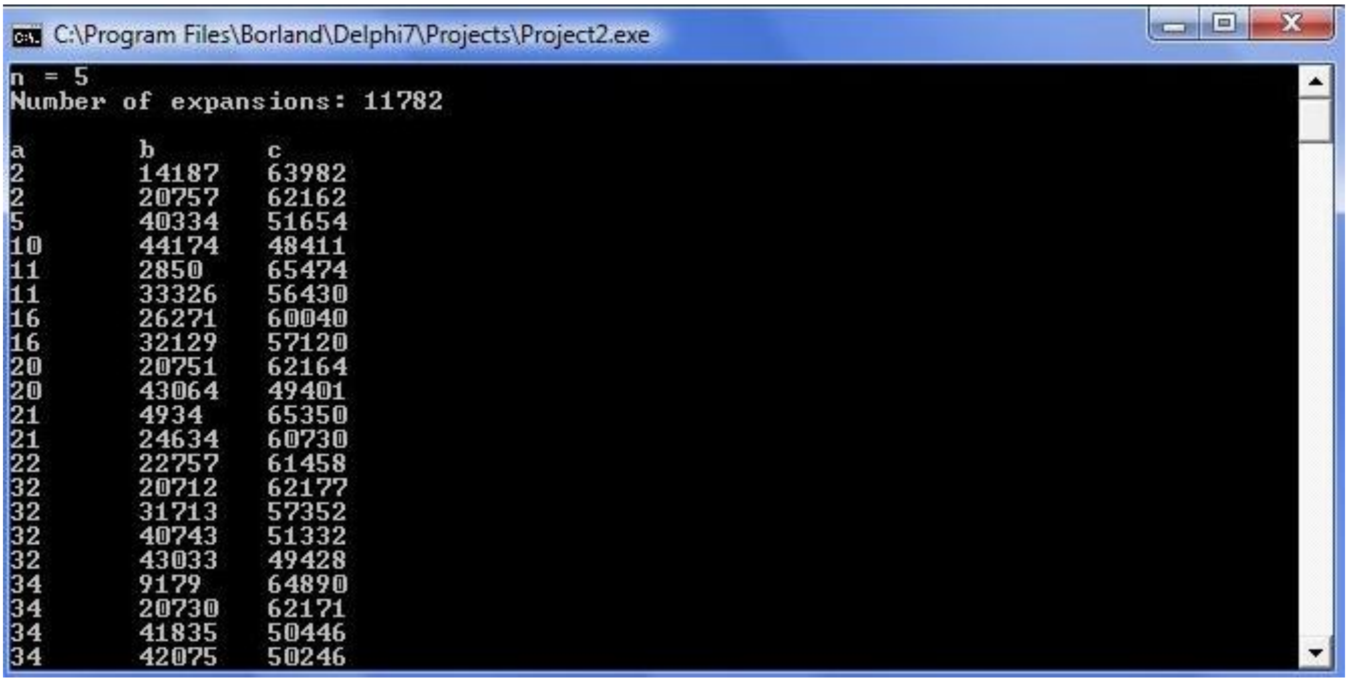
Для $n = 4$ можливих трійок 79.




```
n = 4
Number of expansions: 79

a       b       c
2       142     213
4       89      240
6       50      251
6       74      245
7       108     232
8       63      248
8       168     193
10      114     229
11      30      254
11      54      250
11      70      246
11      146     210
12      143     212
14      171     190
15      76      244
15      164     196
16      159     200
18      133     218
20      56      249
20      84      241
22      162     197
```

Для $n = 5$ можливих трійок 11782.



Очевидно, що простої закономірності, яка дозволяла б оцінити функцію $R_3(F_n)$ не існує (тут $R_3(F_n)$ - функція, що визначає кількість розв'язків $F_n = x^2 + y^2 + z^2$, де $F_n = 2^{2^n} + 1$ - числа Ферма).

В той же час було помічено, що всі числа Ферма взаємно прості, тобто $(F_n; F_k) = 1,\ n \neq k$.

Правильність цього факту випливає із наступної леми.

Лема 1.3.1. Правильна рівність:

$$(1 + x)(1 + x^2) \cdot \ldots \cdot \left(1 + x^{2^{k-1}}\right) = 1 + x + x^2 + \ \ldots + x^{2^{k-1}} \quad (*)$$

Доведення:

Скористаємось методом математичної індукції.

База: $n = 1$. Тоді рівність очевидна.

Нехай $k > 1$. Домножимо ліву і праву частину рівності (*) на $1 + x^2$. Тоді у правій частині до тих членів, що були, додадуться члени, що отримуються при множенні $1, x, x^2, \ldots, x^{2^k - 1}$ на множник x^{2^k}. Тобто x буде входити у всіх степенях від 0 до $2^{k+1} - 1$.

Із припущення індукції: «(*) - істинне», отримана тотожність буде відрізнятись лише тим, що число k змінилось на $k+1$. Тому рівність (*) доведена.

Теорема 1.3.1. $(F_n; F_k) = 1,\ n \neq k.$

Доведення:

Домножимо (*) на $(x-1)$ і покладемо $x = 2$.

$$1 \cdot 3 \cdot \ldots \cdot \left(1 + 2^{2^{k-1}}\right) = 2^{2^k} - 1$$

Додавши до обох частин отриманої рівності 2, маємо:

$$F_1 \cdot F_2 \cdot \ldots \cdot F_k + 2 = F_{k+1} \qquad (**),$$

де $F_{k+1} = 2^{2^k} + 1$.

При $n < k$ число F_n входить у ліву частину рівності (**) одним із множників. Тому найбільший спільний дільник F_n і F_k повинен бути і дільником числа 2, але числа Ферма - непарні. Тому теорема доведена [7].

Подальший розвиток даної проблематики ми вбачаємо у вивченні функції $R_3(F_n)$.

Розділ 2. Заходження кількості коренів деяких діофантових рівнянь методом твірних функцій

2.1. Поняття твірної функції та формального степеневого ряду

Формальним степеневим рядом називаються вираз

$$\alpha(t) = a_0 + a_1 t + a_2 t^2 + \ \ldots + a_n t^n + \ \ldots \qquad (5),$$

де a_i - коефіцієнти ряду, t - формальна змінна ряду.

У даному випадку формальний степеневий ряд (5) є *твірною функцією* для послідовності коефіцієнтів $a_0, a_1, a_2, \ldots, a_n, \ldots$. Проте $\alpha(t)$ не є функцією від змінної t у звичайному розумінні, оскільки $\alpha(t)$ є тільки скороченим записом формального виразу правої частини (5) [6].

Формальні степеневі ряди можна додавати, множити, диференціювати по правилам, аналогічним звичайним правилам додавання, множення, диференціювання скінченних многочленів.

Нехай дані два ряди

$$\alpha(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n + \ldots$$
$$\beta(t) = b_0 + b_1 t + b_2 t^2 + \ldots + b_n t^n + \ldots$$

тоді їх сумою буде

$$\gamma(t) = \alpha(t) + \beta(t) = (a_0 + b_0) + (a_1 + b_1)t + \ldots + (a_n + b_n)t^n + \ldots$$

їх добутком буде

$$\gamma(t) = \alpha(t) \cdot \beta(t) = a_0 b_0 + (a_0 b_1 + a_1 b_0)t + \ldots + (\sum_{i=0}^{n} a_i b_{n-i})t^n + \ldots$$

Диференціюємо ряд $\alpha(t)$ і маємо

$$\gamma(t) = \alpha'(t) = a_1 + 2a_2 t + 3a_3 t^2 + \ldots + n a_n t^{n-1} + \ldots$$

2.2. Кількість коренів рівняння $\boldsymbol{x_1 + x_2 + \ldots + x_m = k}$ в цілих невід'ємних числах

Розглянемо рівняння Ейлера

$$x_1 + x_2 + \ldots + x_m = k \qquad (6),$$

де m і k - певні натуральні числа.

Розглянемо формальний степеневий ряд

$$\alpha(t) = (1 + t + t^2 + t^3 + \ldots)^m \qquad (7)$$

Після розкриття дужок ряду (7) ми отримуємо

$$\alpha(t) = 1 + A_1 t + A_2 t^2 + A_3 t^3 + \ldots$$

Тут коефіцієнт A_k при t^n дорівнює числу способів вибору по одному цілому показнику з кожного множника формального степеневого ряду (7), тобто A_k дорівнює кількості невід'ємних цілих розв'язків рівняння (6). Отже, нашою задачею є розрахунок коефіцієнта A_k.

У формальному степеневому ряді (7) записана сума нескінченної геометричної прогресії. Так як t є формальною змінною, а не числом, то до ряду (7) можна застосувати формулу суми членів нескінченно спадної геометричної прогресії $S=\frac{b_1}{1-q}$, де b_1 - перший член прогресії, а q - знаменник прогресії.

Маємо

$$\alpha(t)=\frac{1}{(1-t)^m}=1+A_1t+A_2t^2+A_3t^3+\ \dots$$

$$\alpha(t)=(1-t)^{-m}=1+A_1t+A_2t^2+A_3t^3+\ \dots \qquad (8)$$

Диференціюємо це рівняння і маємо

$$\alpha'(t)=m(1-t)^{-m-1}=A_1+2A_2t+3A_3t^2+\ \dots$$

Підставимо $t=0$, отримуємо $A_1=m.$ Знову диференціюємо підставляємо $t=0$, отримуємо $A_2=\frac{m(m+1)}{2}$. Продиференціювавши рівняння (8) k разів і підставляючи $t=0$ на кожному кроці ми отримуємо

$$A_k=\frac{m(m+1)\cdot\ldots\cdot(m+k-1)}{k!}=\frac{(m+k-1)!}{(m-1)!\,k!}$$

Очевидно, що отриманий результат ефективний тільки при невеликих значеннях $m.$ В іншому випадку числа стають досить великими, тому доцільно буває оцінити порядок цього числа. Крім того, часто не вдається зайти точну формулу для кількості коренів, але вдається знайти їх оцінку.

2.3. Кількість коренів рівняння $\boldsymbol{a_1x_1+a_2x_2+\ \dots+a_mx_m=n}$ в цілих невід'ємних числах

Розглянемо рівняння

$$a_1x_1+a_2x_2+\ \dots+a_mx_m=n \qquad (9),$$

де a_i, m та n - певні натуральні числа.

Теорема 2.3.1. Рівняння виду (9) має цілі корені тоді і тільки тоді, коли n ділиться на найбільший спільний дільник d коефіцієнтів $a_1, a_2, \dots, a_m$.

Доведення:

Доведемо, що це є необхідною умовою. Дійсно, якщо $x_1, x_2, \dots, x_m$ задовільняють рівняння (9), то d буде дільником кожного добутку $a_1x_1, a_2x_2, \dots, a_mx_m$, а отже і дільником їх суми n.

Доведемо тепер, що це є необхідною умовою. Припустимо, що рівняння (9) має хоча б один цілий корінь. Нехай D - множина всіх натуральних чисел, які задаються наступним чином: число n відноситься до множини D коли існують такі цілі $x_1, x_2, \dots, x_m$, що

$$n = a_1x_1 + a_2x_2 + \dots + a_mx_m \qquad (10)$$

Множина D не є порожньою так як містить хоча б одне число $n = a_1 == a_1 \cdot 1 + a_2 \cdot 0 + \dots + a_m \cdot 0$. Нехай d - найменше натуральне число, що належить множині D (таке число існує, так як у непорожній множині натуральних чисел існує найменше число). Так як $d \in D$, то існують такі цілі $k_1, k_2, \dots, k_m$, що

$$d = a_1k_1 + a_2k_2 + \dots + a_mk_m$$

Але d - найменше число множини D, отже для кожного натурального числа виду (10) виконується нерівність $n \geq d$. Покажемо, що будь-яке число $a_1x_1 + +a_2x_2 + \dots + a_mx_m$ при всіх цілих $x_1, x_2, \dots, x_m$ ділиться на d.

Припустимо, що це твердження не вірне. Тоді при деяких цілих $y_1, y_2, \dots, y_m$ число $a_1y_1 + a_2y_2 + \dots + a_my_m$ при діленні на d має цілу частину s і залишок r. Маємо $a_1y_1 + a_2y_2 + \dots + a_my_m = sd + r$, отже $r = a_1y_1 + a_2y_2 + \dots + a_my_m - -s(a_1k_1 + a_2k_2 + \dots + a_mk_m) = a_1x_1 + a_2x_2 + \dots + a_mx_m$, де $x_i = y_i - sk_i$ при i=1,2…m. Натуральне число r має форму (10), отже $r \in D$. Але $r < d$ так r - залишок при діленні на d. Отримуємо суперечність, так як d - найменше число множини D. Отже, будь-яке число $a_1x_1 + a_2x_2 + \dots + a_mx_m$ при всіх цілих $x_1, x_2, \dots, x_m$ ділиться на d [9], що і треба було довести.

Позначимо через A_n – кількість розв'язків рівняння (9) у цілих невід'ємних числах. Сформулуємо наступну теорему:

Теорема 2.3.2. 1) Твірною функцією для послідовності A_n є функція

$$f(x) = \frac{1}{(1-x^{a_1})\cdot(1-x^{a_2})\cdot\ldots\cdot(1-x^{a_m})}$$

причому A_n дорівнює коефіцієнту при x^n у розкладі цієї функції в степеневий ряд.

2) A_n знаходяться за формулою $A_n = \frac{1}{n!}\cdot f^{(n)}(0)$, де $f^{(n)}(0)$ - значення похідної n-го порядку твірної функції $f(x)$ в точці $x = 0$.

Доведення:

Оскільки $|x| < 1$, то за формулою суми всіх членів нескінченно спадної геометричної прогресії одержуємо

$$\frac{1}{(1-x^{a_1})} = 1 + x^{a_1} + x^{2a_1} + \ \ldots\ , \qquad i = 1, \ldots, m$$

Тоді

$$f(x) = (1 + x^{a_1} + x^{2a_1} + \ \ldots) \cdot (1 + x^{a_2} + x^{2a_2} + \ \ldots) \cdot \ldots \cdot (1 + x^{a_m} + x^{2a_m} + \ \ldots) =$$
$$= 1 + A_1x + A_2x^2 + A_3x^3 + \ \ldots + A_nx^n + \ \ldots$$

Показники при x у першій дужці пробігають усі невід'ємні цілі числа, кратні a_1, у другій - кратні a_2, і т.д., у m-й - кратні a_m. Зрозуміло, що після розкриття дужок (без зведення подібних доданків) доданок x^n, увійде в загальну суму стільки разів, скільки існує цілих невід'ємних розв'язків рівняння (9). За домовленістю їх A_n, тому коефіцієнтом при x^n в кінцевому ряді буде саме число A_n.

Щоб одержати формулу для обчислення A_n, знайдемо похідні:

$$f'(x) = A_1 + 2A_2x + 3A_3x^2 + \ \ldots + nA_nx^{n-1} + \ \ldots$$

$$f''(x) = 2\cdot 1A_2 + 3\cdot 2A_3x + \ \ldots + n\cdot(n-1)A_nx^{n-2} + \ \ldots$$

$$\vdots$$

$$f^{(n)} = n\cdot(n-1)\cdot\ldots\cdot 2\cdot 1A_n + \cdots + (n+1)\cdot n\cdot(n-1)\cdot\ldots\cdot 2A_{n+1}x + \ \ldots$$

Звідси $f^{(n)}(0) = n!\,A_n$, тобто $A_n = \frac{1}{n!}\cdot f^{(n)}(0)$.

Таким чином доведено, що $R_n = A_n = \frac{f^{(n)}(0)}{n!}$ (12)

Отже, залишилось зробити оцінку (12), оскільки явно записати формулу, згідно такого підходу до розв'язання зразу не вдається.

Розділ 3. Діофантове рівняння виду $\boldsymbol{a_1 x_1 + a_2 x_2 + \ldots + a_m x_m = n}$

3.1. Круговий метод Харді-Літлвуда

Отримана в попередньому розділу формула (12) не вказує як можна одержати кількість коренів в загальному вигляді. В той же час часто буває важливим просто оцінити їхню кількість. Розв'язати цю проблему можна скориставшись круговим методом Харді-Літлвуда.

Позначимо аналітичне продовження твірної функції (12) на комплексну область $|z| < R$ як $\varphi(z)$. Якщо функції $\varphi(z)$ є аналітичною в області $|z| < R$, то її можна почленно диференціювати в цій області потрібне число раз і на підставі теорем Коші і Тейлора (ТФКЗ) справедлива формула

$$A_n = Res[\varphi(z)/z^{n+1}, 0] = \frac{1}{n!}\lim_{z\to 0}\varphi(z) = \frac{1}{2\pi i}\int_{|z|<R}\varphi(z)dz/z^{n+1}$$

Так як твірна функція (12) є аналітичною при $|z| < 1$, то

$$R_n = A_n = \frac{1}{2\pi i}\int_{|z|<1} dz/z^{n+1}\,(1-z^{a_1})(1-z^{a_2})\cdot\ldots\cdot(1-z^{a_m})$$

Інтеграли можна знаходити за допомогою лишків для отримання кількості розв'язків рівняння (9) при невеликих значеннях n.

3.2. Рівняння виду $\boldsymbol{x_1 + 2x_2 + 3x_3 + \ldots + nx_n = n^2}$

Розглянемо рівняння виду

$$x_1 + 2x_2 + 3x_3 + \ldots + nx_n = n^2 \qquad (13)$$

Рівняння (13) є модифікацією загального рівняння (9), тому використовуючи твірну функцію і круговий метод Харді-Літлвуда теоретично можна знайти R_n у явному вигляді.

На даний момент [5] відома асимптотична оцінка знизу і зверху для функції R_n:

$$\frac{n^n(n-1)^{n-1}}{2^{n-1}(n!)^2} < R_n < \frac{n^{2n-1}}{(n!)^2} \qquad (14)$$

Наразі нам не відомо чи можна покращити цю оцінку, тому ми пропонуємо вирішити це питання опосередковано. Виходячи із специфіки правої частини (13) (повний квадрат) сформулюємо гіпотезу.

Гіпотеза 3.2.1. Кількість коренів рівняння (13) дорівнює кількості впорядкованих способів представлення числа n^2 сумою n непарних чисел.

Кількість коренів рівняння (13) можна знайти за допомогою побудови наступної таблиці:

Таблиця 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1														
2	1	1													
3	1	1	1												
4	1	2	1	1											
5	1	2	2	1	1										
6	1	3	3	2	1	1									
7	1	3	4	3	2	1	1								
8	1	4	5	5	3	2	1	1							
9	1	4	7	6	5	3	2	1	1						
10	1	5	8	9	7	5	3	2	1	1					
11	1	5	10	11	10	7	5	3	2	1	1				
12	1	6	12	15	13	11	7	5	3	2	1	1			
13	1	6	14	18	18	14	11	7	5	3	2	1	1		
14	1	7	16	23	23	20	15	11	7	5	3	2	1	1	
15	1	7	19	27	30	26	21	15	11	7	5	3	2	1	1

Для кожного n кількість коренів знаходиться у клітинці $a[\frac{n(n+1)}{2}, n]$. Для побудови внесемо $a[1,1] = 1$, а далі будемо заповнювати за правилом

$$a[i,j] = \sum_{k=1}^{j} a[i-j,k]$$

Шляхом створення комп'ютерної програми «MatrixBuild» методом комп'ютерного перебору ми встановили кількість коренів для деяких n. Розроблена програма представлена у Додатку2.

Приведемо дані для оцінки R_n за (14) і за результатами значень R_n згідно *таблиці 1*.

Таблиця 2

Висновки

Дана дослідницька робота складається із вступу, трьох розділів, висновків, списку використаних джерел та додатку.

В першому розділі роботи наведено огляд результатів з проблем теорії адитивних чисел. У ньому наведені формули одного з розв’язків рівняння $F_n = x^2 + y^2 + z^2$, де $F_n = 2^{2^n} + 1$ - числа Ферма, а саме

$$\begin{cases} a = \dfrac{2 \times 2^{2^{n-1}} + 1}{3} \\ b = \dfrac{2^{2^{n-1}} + 2}{3} \\ c = \dfrac{2 \times 2^{2^{n-1}} - 2}{3} \end{cases}$$

У другому розділі ми розглянули формальні степеневі ряди та твірні функції. Крім того, застосували їх для оцінки коренів рівнянь (6) і (9). Для рівняння (6) отримана зручна формула, яка дозволяє обчислювати кількість його коренів (A_k) при будь-яких m та k, а саме

$$A_k = \frac{m(m+1)\cdot\ldots\cdot(m+k-1)}{k!} = \frac{(m+k-1)!}{(m-1)!\,k!}$$

Для рівняння (9) отримана формула (12) дає можливість обчислення кількість його коренів (A_k) при невеликих значеннях n та m, тому у третьому розділі вказано на теоретичну можливість покращення оцінки кількості коренів рівняння (9), використовуючи формулу

$$A_n = \frac{1}{2\pi i}\int_{|z|<1} dz/z^{n+1}\,(1-z^{a_1})(1-z^{a_2})\cdot\ldots\cdot(1-z^{a_m})$$

Була сформульована гіпотеза та створена програма для знаходження кількості коренів рівняння

$$x_1 + 2x_2 + 3x_3 + \ \ldots + nx_n = n^2$$

Окреслили шлях у дослідженні можливості покращити оцінку (14).

Таким чином в результаті проведеного дослідження ми:

1) одержали формули, що дозволяють розв'язати діофантове рівняння $F_n = x^2 + y^2 + z^2$ в двійковій і десятковій системах числення;

2) одержали формулу кількості коренів рівняння $x_1 + x_2 + \ \ldots + x_m = k$ в цілих невід'ємних числах;

3) одержали формулу кількості коренів рівняння $a_1x_1 + a_2x_2 + \ldots + a_mx_m = n$ в цілих невід'ємних числах;

4) довели оцінку кількості коренів рівняння $x_1 + 2x_2 + 3x_3 + \ \ldots + nx_n = n^2$ і створили програму для безпосереднього знаходження функції R_n.

Робота носить теоретичний характер. Результати роботи і методика їх застосування можуть бути використані при розв'язуванні задач теорії чисел.

Список використаних джерел

1. Безущак О.О., Ганюшкін О.Г Елементи теорії чисел. Київ: Вид-во КНУ, 2003, 202с.
2. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981. – 176с.
3. Ожигова Е. П. Что такое теория чисел, – М ., «Знание», 1970. – 95с.
4. Завдання для відбірних етапів XVII-го Всеукраїнського турніру юних математиків імені професора М. Й. Ядренка. [Електронний ресурс]: офіц. веб-портал The over-ukrainian tournament of young mathematicians named after prof. Mykhailo Yadrenko – Режим доступу: https://dl.dropboxusercontent.com/u/15765938 /TYM/2014/TYM-2014-LYST_PROBLEMS.pdf
5. Завдання для відбірних етапів XIX-го Всеукраїнського турніру юних математиків імені професора М. Й. Ядренка. [Електронний ресурс]: офіц. веб-портал The over-ukrainian tournament of young mathematicians named after prof. Mykhailo Yadrenko – Режим доступу: https://dl.dropboxusercontent.com/u/15765938

/TYM/2016/LYST_IMZO_ZAVDANNYA_XIX_TYM.pdf

6. Квант / Капица С. П. // М.: Наука, 1984. – № 5. – С. 11-15.

7. Рябухо О.М. Дослідження імовірнісних алгоритмів тестування простоти чисел / О.М. Рябухо, Т.В. Турка // Збірник наукових праць фізико-математичного факультету ДДПУ. – 2013. – Випуск 3. – С. 60–67.

8. Савин А. П. Энциклопедический словарь юного математика - М.: Педагогика, 1989. – С. 95-96. [Електронний ресурс]. – Режим доступу: http://sernam.ru/book_e_math.php?id=37&filter=images&num=91

9. Серпінський В. Ф. О решении уравнений в целых числах. – М.: Физматлит, 1961 – 88с.

Додатки

Додаток1. ***«Search triples»***

Програма пошуку трійок для рівняння вигляду $\boldsymbol{F_n = x^2 + y^2 + z^2}$ «Search triples»
Код програми пошуку:

```
Program SearchTriples;
{$APPTYPE CONSOLE}

uses
  SysUtils, Math;

var
  n, a, b, t, m, k, c, res: uint64;
begin
  res := 0;
  write('Enter n: ');
  readln(n);
  m := round(intpower(2, round(power(2, n)))) + 1;
  writeln('2^2^n + 1 = ', m);
  t := round(power(m/3,0.5));
  a := 0;
```

```
while a <= t do
begin
  inc(a);
  b := a;
  k := round(power((m-intpower(a,2))/2,0.5));
  while b <= k do
  begin
    inc(b);
    c := m - round(intpower(a,2) + intpower(b,2));
    if (c >= 1) and (round(power(c,0.5))>b) and
(round(intpower(round(power(c,0.5)),2)) = c) then begin
      inc(res);
      writeln(res, #9, #9, a, #9, b, #9, round(power(c,0.5)));
    end;
  end;
end;
writeln('Number of expansions: ', res);
readln;readln;
end.
```

Додаток2. ***«MatrixBuild»***

Програма для пошуку кількості коренів рівняння виду
$x_1 + 2x_2 + 3x_3 + \ ... \ + nx_n = n^2$ «MatrixBuild»
Код програми пошуку:

```
Program MatrixBuild;

uses Math;


Var n, s : uint64;

    snr, i, j, k : longint;

    a : array [1..5050, 1..100] of uint64;


begin

  Write( 'n = ' );

  Readln( n );
```

```
  snr:=(n*(n+1)) shr 1;
  For i:=1 to snr do
    begin
      a[i,1]:=1;
      a[i,i]:=1;
    end;
  For i:=2 to snr do
    For j:=2 to min(n,i-1) do
      begin
        s:=0;
        For k:=1 to j do
          s:=s+a[i-j,k];
        a[i,j]:=s;
      end;
  Writeln( 'R(', n, ') = ', a[snr,n] );
end.
```