République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Djilali BOUNAÂMA Khemis Miliana

Mémoire Présenté

Pour l'obtention de diplôme de

Master en Mathématiques

Spécialité : Analyse Mathématiques et Applications

Intitulé

Sommes de quatre nombres polygonaux avec des coefficients

Réalisé par : **Bensmaili Kamel Eddine** Soutenu publiquement le : 14 Septembre 2017

devant les membres du jury :

Mr. M. Karras	Université de Djilali BOUNAÂMA.	Président
Mr. M. Houasni	Université de Djilali BOUNAÂMA	Encadrant
Mr. B. Saadaoui	Université de Djilali BOUNAÂMA	Examinateur
Mr. M. Bouderbala	Université de Djilali BOUNAÂMA	Examinateur

Année Universitaire 2016/2017

Dédicaces

Ce travail est dédié :

À mon cher père et chère mère

À mes très chers frères et sœurs

À mes chères amies

Remerciements

Je remercie Allah, le tout puissant, le Miséricordieux, qui nous a donne l'opportunité de mener à bien ce travail.

C'est avec un grand plaisir que, j'adresse mes sincères remerciements à mon encadreur, Monsieur Mohamed Houasni pour ces conseils et son suivi durant la réalisation de ce travail.

Je tiens remercie également les nombres du jury qui ont bien voulu s'examiner ce travail.

À mon cher père : qui a toujours cru en moi et a mis a ma disposition tous les moyens nécessaires pour que je réussisse dans mes études.

À ma chère mère : que je ne cesse de remercier pour tout ce qu'elle m'a donné. Elle m'a supporté dans son ventre 9 mois. Qu'Allah le récompense pour tous ces bienfaits.

À mes très chers frères Abdelhak et Mohamed

À mes chères amies :Omar,Othman, Yacine et Karima Adoum,Fatiha, Youssef, Benmira, Abdelkader,Chahrazad, , et Souad : en souvenir des moments agréables passés ensemble, veuillez trouver dans ce travail l'expression de ma tendre affection et mes sentiments les plus respectueux avec mes vœux de succès, de bonheur et de bonne santé.

À tous ceux ou celles qui me sont chers et que j'ai omis involontairement de citer.

À tous mes enseignants tout au long de mes études.

À tous ceux qui ont participé de près ou de loin à la réalisation de ce travai

Mes remerciements aussi à tous mes professeurs qui ont contribué à mon information.

Je ne terminai pas sans avoir exprimé des remerciements envers toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce travail.

Notations

$\mathbb{N}$	L'ensemble des nombres naturels.
$\mathbb{Z}$	L'ensemble des nombres entiers.
$\mathbb{Z}^+$	L'ensemble des nombres entiers structement positifs $\mathbb{Z}^+ = \{1, 2, 3, ...\}$.
$\mathbb{Z}/n\mathbb{Z}$	Les classes résiduelles d'entiers modulo n.
$a \equiv b (\bmod n)$	a congrus b modulo n (n divise $a - b$)
$PPCM(a, b)$	Le plus petit commun multiple de a et b.
φ	La fonction indicatrice d'Euler.
$PGCD(a, b)$	Le plus grand commun deviseur de a et b.
$a \mid b$	a est divise b.
$\deg(g(x))$	Degré de polynôme $g(x)$.
$p \nmid n$	signifié p n'est pas diviseur de n.
$p^\alpha \parallel n$	$p^\alpha \mid n$ et $p^{\alpha+1} \nmid n$.
$\left(\frac{a}{b}\right)$	symbole de Legendre

Table des matières

Introduction

Les nombres polygonaux d'ordre $m + 2$ ($m \in \mathbb{Z}^+$) sont des nombres qui sont construits géométriquement à partir des polygones réguliers avec $m + 2$ côtés, ils sont donnés par

$$P_{m+2}(n) = m \begin{pmatrix} n \\ 2 \end{pmatrix} + n = \frac{mn^2 - (m-2)\,n}{2}$$

pour $n \in \mathbb{N}$.

La conjecture célèbre de Fermat prouvée en 1847 par Cauchy affirme que chaque entier naturel b est la somme de $m + 2$ nombres polygonaux d'ordres $m + 2$ a été prouvé par Lagrange dans le cas $m = 2$, Gauss dans le cas $m = 1$ et Cauchy dans le cas $m > 3$ (voir [9, pp. 3-35] et [7,pp. 54-57]).

En 1830, Legendre affine le théorème du nombre polygonal de Cauchy en montrant que tout entier $N > 28m^3$ avec $m > 3$ peut être écrit comme

$$P_{m+2}(x_1) + P_{m+2}(x_2) + P_{m+2}(x_3) + P_{m+2}(x_4) + \delta_m(N)$$

avec $x_1, x_2, x_3, x_4 \in \mathbb{N}$, telle que $\delta_m(N) = 0$ si $2 \nmid m$, et $\delta_m(N) \in \{0, 1\}$ si $2 \mid m$.

En 1917, Ramanujan [10] a répertorié tous les 54 quadruples possibles (a, b, c, d) de nombres entiers positifs où

$$a \leq b \leq c \leq d$$

tels que n'importe quel $n \in \mathbb{N}$ peut être écrit comme

$$ax^2 + by^2 + cz^2 + dw^2, \text{ avec } x, y, z, w \in \mathbb{Z}.$$

Récemment, Sun [12] a montré que tout entier positif peut être écrit comme somme de quatre nombres octogonaux généralisés dont l'un est impair. Il a aussi prouvé que pour plusieurs triples (b, c, d) d'entiers positifs ($(1, 1, 3), (1, 2, 2)$ et $(1, 2, 4)$),

on a

$$\{P_8(x_1) + bP_8(x_2) + cP_8(x_3) + dP_8(x_4) : x_1, x_2, x_3, x_4 \in \mathbb{Z}\} = \mathbb{N}.$$

Dans [12, Conjecture 5.3], Sun a conjecturé que tout $n \in \mathbb{N}$ peut être écrit comme

$$P_6(x_1) + p_6(x_2) + 2p_6(x_3) + 4p_6(x_4)$$

avec $x_1, x_2, x_3, x_4 \in \mathbb{N}$.

Motivé par le travail ci-dessus, pour $(a, b) = (1, 1)$, $(2, 2)$, $(1, 3)$, $(2, 4)$ et $m \in \{3, 4, 5, ...\}$, nous étudions si un entier suffisamment grand peut être écrit comme

$$P_{m+2}(x_1) + P_{m+2}(x_2) + aP_{m+2}(x_3) + bP_{m+2}(x_4) \tag{1}$$

pour

$$(a, b) = (1, 1), (2, 2), (1, 3), (2, 4) \text{ et } m \in \{3, 4, 5, ...\}$$

avec $x_1, x_2, x_3, x_4 \in \mathbb{N}$.

Ce mémoire comporte deux chapitres

Le premier chapitre est consacré aux définitions et notations qui sont utiles pour la suite de ce travail.

Le deuxième chapitre est consacré à l'étude des cas (a, b) dans la formule 1 précédente.

Chapitre 1

Généralités

Dans ce chapitre, nous allons exposer un ensemble des notions de base utiles, nous présentons des définitions et quelques théorèmes fondamentaux concernant les nombres polygonaux, congruences, symbole de Lagrange, théorème de Dirichlet et de Gauss.

1.1 Définitions

Définition 1 *Un nombre figuré est un nombre qui peut être représenté par un ensemble de points disposés de façon plus ou moins régulière et formant une figure géométrique.*

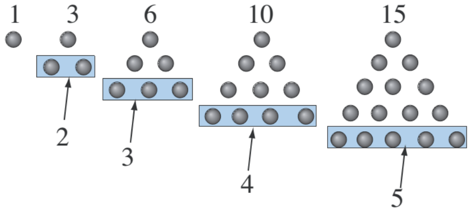
Définition 2 *un polygone régulier est un polygone à la fois équilatéral (tous ses côtés ont la même longueur) et équiangle(tous ses angles ont la même mesure).*

Définition 3 *un nombre polygonal est un nombre figuré qui peut être représenté par un polygone régulier.*

1.2 Exemples

1.2.1 Nombres triangulaires

Les nombre triangulaires sont ceux que l'on peut disposer de façon à former un triangle comme dans l'illustration suivant



Les premiers nombres triangulaires sont

$$P_3(1) \quad = 1,\ P_3(2) = 3 = 1 + 2,\ P_3(3) = 6 = 1 + 2 + 3,\ P_3(4) = 10 = 1 + 2 + 3 + 4,$$

et par suite:

$$P_3(n) = 1 + 2 + 3 + ...n$$

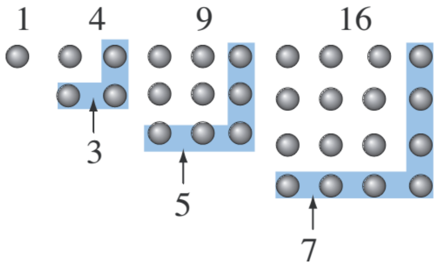
$P_3(n)$ est une somme de suite arithmétique, alors

$$P_3(n) = \frac{n + n^2}{2},$$

est le n-ième nombre triangulaire.

1.2.2 Nombres carrés

Les nombres carrés sont ceux que l'on peut disposer de façon à former un carré comme dans l'illustration suivante



on remarque que

$$P_4(1) = 1,\ P_4(2) = 4 = 1 + 3,\ P_4(3) = 9 = 1 + 3 + 5,\ P_4(4) = 16 = 1 + 3 + 5 + 7,$$

et par suite le n-ième nombre carré est une somme de suite arithmétique

$$P_4(n) = 1 + 3 + 5 + ...2n - 1 = n^2.$$

Proposition 1 *la somme de deux nombres triangulaires successif* $P_3(n-1)$ *et* $P_3(n)$ *égale le nombre carré* $P_4(n)$ *.*

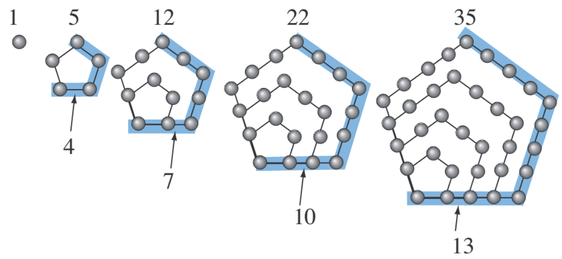
Preuve. ona

$$P_3(n-1) + P_3(n) = \frac{n^2+n}{2} + \frac{(n-1)^2+n-1}{2} = n^2.$$

■

1.2.3 Nombres pentagonaux

Les premiers nombres pentagonaux sont



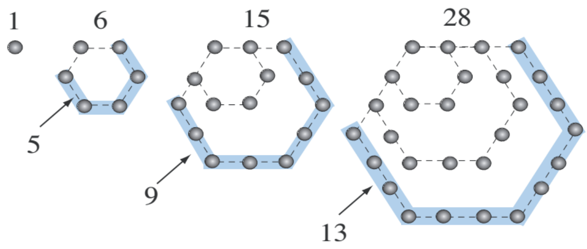
$$P_5(1) = 1, \quad P_5(2) = 5 = 1 + 4, \quad P_5(3) = 12 = 1 + 4 + 7, \quad P_5(4) = 22 = 1 + 4 + 7 + 10$$

et par suite le n-ième nombre pentagonaux est une somme de suite arithmétique

$$P_5(n) = 1 + 4 + 7 + ...3n - 2 = \frac{3n^2 - n}{2}$$

1.2.4 Nombres hexagonaux

Les premiers nombres hexagonaux sont



on a

$$P_6(1) = 1,\ P_6(2) = 6 = 1 + 5,\ P_6(3) = 15 = 1 + 5 + 9,\ P_6(4) = 28 = 1 + 5 + 9 + 13,$$

et par suite le n-ième nombre hexagonaux est une somme de suite arithmétique

$$\begin{aligned} P_6(n) &= 1 + 5 + 9 + ...4n - 3 = \frac{4n^2 - 2n}{2} \\ &= 2n^2 - n. \end{aligned}$$

1.2.5 Nombres (m + 2)-gonaux

Proposition 2 *soit $m \in \mathbb{Z}^+$, la forme générale d'un nombre polygonal à $m + 2$ côtés de rang n est donnée par l'expression suivante:*

$$P_{m+2}(n) = \frac{mn^2 - (m-2)n}{2}.$$

Définition 4 *n représente la longueur de chaque coté du polygone.*

Preuve. pour $m = 1$, on a

$$P_3(n) = 1 + 2 + 3 + ...n,$$

et pour $m = 2$, on a

$$P_4(n) = 1 + 3 + 5 + ...2n - 1;$$

supposons que

$$P_{m+2}(n) = 1 + (m + 1) + (m + 2) + ...m(n - 1) + 1,$$

alors

$$\begin{aligned} P_{m+3}(n) &= 1 + (m+2) + (m+3) + ...m(n-1) + n \\ &= \frac{(m+1)n^2 - (m-1)n}{2}, \end{aligned}$$

donc, par récurrence on obtient

$$P_{m+2}(n) = \frac{mn^2 - (m-2)n}{2}.$$

■

Propriétés 1 *Soit $m \in \mathbb{Z}^+$, et $n \in \mathbb{N}$, on a les relations suivantes*

$$\begin{aligned} P_3(2n) &= 3P_3(n) + P_3(n-1) \\ P_4(n) &= P_3(n) + P_3(n-1) \\ P_4(2n+1) &= 8P_3(n) + 1 \\ P_6(n) &= P_3(n) + 3P_3(n-1) \\ P_6(n) &= P_3(2n-1) \\ P_8(n) &= 6P_3(n-1) + n \\ P_{m+2}(n) &= (m-1)P_3(n-1) + P_3(n) \\ P_{m+2}(n) &= P_{m+1}(n) + P_3(n-1). \end{aligned}$$

1.3 Congruences dans l'anneau $\mathbb{Z}$

Historiquement, la notion de congruence sur les entiers relatives a été introduite par Gauss vers 1801. Si a et b sont deux entiers et si $n \geq 2$ est un entier, on convient d'écrire:
$a \equiv b \,(\mathrm{mod}\, n)$ si et seulement si $a - b \in n\mathbb{Z}$. On dit alors que les entiers a et b sont congrus modulo $n\mathbb{Z}$. La relation de congruence modulo n ainsi définie est une relation d'équivalence définie sur l'anneau $\mathbb{Z}$, compatible avec l'addition et la multiplication définies sur $\mathbb{Z}$. Voici maintenant le théorème principal d'arithmétique qui nous sera utile.

1.3.1 Fonction indicatrice φ d'Euler et le théorème d'Euler

Définition 5 *On appelle fonction arithmétique toute fonction définie sur l'ensemble des entiers naturels non nuls $\mathbb{N}^*$ à valeurs dans l'ensemble des nombres complexes $\mathbb{C}$. La fonction indicatrice d'Euler que l'on note φ, est une fonction arithmétique importante. Elle est définie comme suit*

$$\varphi(n) = \mathrm{Card}\left\{m \in \mathbb{N}^* \;/\; 1 \leq m < n \;\textit{ et }\; \mathrm{pgcd}(n,m) = 1\right\}.$$

Théorème 1 *Pour tout entier $n \geq 2$ et pour tout entier a, tels que $PGCD\,(a,n) = 1$, on a*

$$a^{\varphi(n)} \equiv 1 \pmod n \cdot$$

Preuve. Soit U_n l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

$$U_n = \left\{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_{\varphi(n)}}\right\}, \quad x_i \neq x_j \text{ pour } i \neq j,$$

et soit

$$V_n = \left\{\overline{ax_1}, \overline{ax_2}, \ldots, \overline{ax_{\varphi(n)}}\right\},$$

tous les x_i sont premiers avec n ainsi que a, donc quelque soit i, $\overline{ax_i}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et $V_n \subset U_n$. De même si $i \neq j$, $\overline{ax_i} \neq \overline{ax_j} \Longleftrightarrow \overline{a}\left(\overline{x_i - x_j}\right) \neq \overline{0}$, puisque $\overline{a}$ est inversible et $\overline{x_i} \neq \overline{x_j}$ On a donc cardV_n =cardU_n et $V_n = U_n$. On peut ainsi écrire

$$\prod_{i=1}^{\phi(n)} \overline{x_i} = \prod_{i=1}^{\phi(n)} \overline{ax_i},$$

ce qui peut aussi s'écrire

$$\prod_{i=1}^{\phi(n)} \overline{x_i} = \overline{a^{\phi(n)}} \prod_{i=1}^{\phi(n)} \overline{x_i},$$

comme $\prod_{i=1}^{\phi(n)} \overline{x_i}$ est premier avec n, on obtient par simplification

$$a^{\phi(n)} \equiv 1 \pmod n.$$

■

1.4 Quelques théorèmes

Définition 6 *Soit A une matrice symétrique*

$$A = (a_{i,j})_{n \times n},$$

la forme quadratique F_A est

$$F_A\,(x_1, x_2, \ldots x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} x_i x_j,$$

tels que F_A est une fonction de deuxième degré avec n variables $x_1, x_2, \ldots x_n$,

$$F_A\,(x_1, x_2, \ldots x_n) = x_1^2 + x_2^2 \ldots + x_n^2.$$

Définition 7 *soient $a \in \mathbb{Z}$ et $m \in \mathbb{Z}^{+}$,on dit que a est residue quadratique modulo m s'il existe $x, y \in \mathbb{Z}$ tels que*

$$x^2 - a = ym. \text{ ou } \ x^2 \equiv a \pmod m$$

Définition 8 *soit p est un nombre premier et $a \in \mathbb{Z}$ un entier tels que*

$$PGCD\,(a,p) = 1,$$

alors le symbole de Legendre $\left(\dfrac{a}{p}\right)$ est définit comme suit

i) 0 si a est divisible par p ;

ii) 1 si a est un résidu quadratique modulo p;

iii) -1 si a n'est pas un résidu quadratique modulo p.

Théorème 2 [*cf*([9] , *p*18)]*on trouve $n \in \mathbb{N}$ tels que $n \geq 2$, s'il existe un nombre entier positive d tels que $-d$ est un residue quadratique modulo $dn - 1$*

alors on peut écrire n sous la forme d'une somme de trois nombres carrés.

Théorème 3 (Dirichlet) [*cf*([9] , *p*98)] *on trouve $\alpha, Q \in \mathbb{R}$, avec $Q \geq 1$, alors il existe $a, q \in \mathbb{Z}$ tels que*

$$1 \leq q \leq Q \text{ avec } PGCD\,(a,q) = 1, \text{ et } \left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qQ}.$$

Lemme 1 *Soit n est un entier positive tels que*

$$n \equiv 2 \pmod 4,$$

alors on peut écrire n comme somme de trois nombres carrés.

Preuve. On a

$$PGCD\,(4n, n-1) = 1,$$

alors, il existe une infinité des nombres premiers

$$p \in \{4nj + n - 1 : j = 1, 2...\},$$

tels que

$$p = 4nj + n - 1 = (4j+1)\,n - 1,$$

soit

$$d = 4j + 1,$$

on a

$$n \equiv 2 \pmod 4,$$

alors

$$p = dn - 1 \equiv 1 \pmod 4,$$

d'après le théorème 2,il suffit de démontrer que $-d$ est un residue quadratique modulo p

soit

$$d = \prod_{q_i|d} q_i^{k_i},$$

tels que q_i sont les nombres premiers qui divisent d, alors

$$p = dn - 1 \equiv -1 \pmod{q_i},$$

pour tout i, et

$$d \equiv \prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} \equiv 1 \pmod 4,$$

donc

$$\prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} = 1,$$

d'après la définition 8 on a

$$\left(\frac{-1}{p}\right) = 1,$$

comme $p \equiv 1 \pmod 4$

alors

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right),$$

$$= \left(\frac{d}{p}\right),$$

et on a

$$\left(\frac{-d}{p}\right) = \prod_{q_i|d}\left(\frac{q_i}{p}\right)^{k_i},$$

$$= \prod_{q_i|d}\left(\frac{p}{q_i}\right)^{k_i} = \prod_{q_i|d}\left(\frac{-1}{q_i}\right)^{k_i},$$

$$= \prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i} = 1,$$

donc $-d$ est un residue quadratique modulo p, alors n est un somme de trois nombres carrés ■

Lemme 2 *Soit n un entier positive tels que*

$$n \equiv 1, 3 \text{ ou } 5 \pmod 8,$$

alors on peut écrire n comme somme de trois nombres carrés.

Preuve. Il est clair que 1 est un somme de trois nombres carrés.

Soit $n \geq 2$ et soit

$$c = \begin{cases} 3 & \text{si } n \equiv 1 \pmod 8 \\ 1 & \text{si } n \equiv 3 \pmod 8 \\ 3 & \text{si } n \equiv 5 \pmod 8 \end{cases},$$

si $n \equiv 1$ ou $3 \pmod 8$, alors

$$\frac{cn-1}{2} \equiv 1 \pmod 4,$$

si $n \equiv 5 \pmod 8$, alors

$$\frac{cn-1}{2} \equiv 3 \pmod 4,$$

pour tout les cas

$$PGCD\left(4n, \frac{cn-1}{2}\right) = 1,$$

d'après le théorème 3 (*Dirichlet*),il existe un nombre premier p de la forme

$$p = 4nj + \frac{cn-1}{2}, \text{ pour } j \in \mathbb{Z}^{+}.$$

Soit

$$d = 8j + 1,$$

alors

$$2p = (8j + c)\, n - 1 = dn - 1,$$

d'après le théorème 2,il suffit de démontrer que $-d$ est un residue quadratique modulo $2p$

si $-d$ est un residue quadratique modulo p,

alors il existe $x_0 \in \mathbb{Z}$ tels que

$$(x_0 + p)^2 + d \equiv 0 \pmod{p}.$$

Soit $x = x_0$ si x_0 est impair et Soit $x = x_0 + p$ si x_0 est pair

alors x est impair et $x^2 + d$ est pair,

et on a

$$x^2 + d \equiv 0 \pmod{2},$$

et

$$x^2 + d \equiv 0 \pmod{p},$$

alors

$$x^2 + d \equiv 0 \pmod{2p},$$

donc, il suffit de démontrer que $-d$ est un residue quadratique modulo p

soit

$$d = \prod_{q_i | d} q_i^{k_i},$$

tels que q_i sont les nombres premiers qui divise d

on a

$$2p \equiv -1 \pmod{d},$$

et par suite

$$2p \equiv -1 \pmod{q_i},$$

et

$$PGCD\,(p,q_i)=1.$$

Si $n\equiv 1$ ou $3 \pmod 8$, alors

$$p\equiv 1 \pmod 4$$

et

$$\left(\frac{-d}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{d}{p}\right)=\left(\frac{d}{p}\right)$$

$$=\prod_{q_i|d}\left(\frac{q_i}{p}\right)^{k_i}=\prod_{q_i|d}\left(\frac{p}{q_i}\right)^{k_i}.$$

Si $n\equiv 5 \pmod 8$, alors

$$p\equiv 3 \pmod 4,$$

et

$$d\equiv 3 \pmod 8,$$

on obtient

$$d=\prod_{\substack{q_i\,|\,d\\ q_i\equiv 1\,(\mathrm{mod}\,4)}} q_i^{k_i}\prod_{\substack{q_i\,|\,d\\ q_i\equiv 3\,(\mathrm{mod}\,4)}} q_i^{k_i},$$

$$\equiv\prod_{\substack{q_i\,|\,d\\ q_i\equiv 3\,(\mathrm{mod}\,4)}}(-1)^{k_i} \pmod 8,$$

$$\equiv -1 \pmod 4,$$

alors

$$\prod_{\substack{q_i\,|\,d\\ q_i\equiv 3\,(\mathrm{mod}\,4)}}(-1)^{k_i}=-1,$$

d'après la définition 2 on a

$$\left(\frac{-1}{p}\right) = -1,$$

alors

$$\begin{aligned}
\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = -\left(\frac{d}{p}\right), \\
= - \prod_{\substack{q_i \mid d \\ q_i \equiv 1 \pmod 4}} \left(\frac{q_i}{p}\right) \prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 4}} \left(\frac{q_i}{p}\right)^{k_i} \\
= - \prod_{\substack{q_i \mid d \\ q_i \equiv 1 \pmod 4}} \left(\frac{p}{q_i}\right) \prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 4}} \left(\frac{p}{q_i}\right)^{k_i} \prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 4}} (-1)^{k_i}, \\
= \prod_{\substack{q_i \mid d \\ q_i \equiv 1 \pmod 4}} \left(\frac{p}{q_i}\right) \prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 4}} \left(\frac{p}{q_i}\right)^{k_i}, \\
= \prod_{q_i \mid d} \left(\frac{p}{q_i}\right),
\end{aligned}$$

alors dans les deux cas on a

$$\left(\frac{-d}{p}\right) = \prod_{q_i \mid d} \left(\frac{p}{q_i}\right),$$

$$= \prod_{q_i \mid d} \left(\frac{2}{q_i}\right)^{k_i} \prod_{q_i \mid d} \left(\frac{2p}{q_i}\right)^{k_i},$$

$$= \prod_{q_i \mid d} \left(\frac{2}{q_i}\right)^{k_i} \prod_{q_i \mid d} \left(\frac{-1}{q_i}\right)^{k_i},$$

$$\left(\frac{-d}{p}\right) = \prod_{\substack{q_i \mid d \\ q_i \equiv 3,5 \pmod 8}} (-1)^{k_i} \prod_{\substack{q_i \mid d \\ q_i \equiv 3,7 \pmod 8}} (-1)^{k_i},$$

$$= \prod_{\substack{q_i \mid d \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i},$$

alors $-d$ est un residue quadratique modulo $2p = dn - 1$

si

$$\sum_{\substack{q_i \mid d \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2,$$

on a

$$d = \prod_{\substack{q_i \mid d \\ q_i \equiv 1 \pmod 8}} q_i^{k_i} \prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 8}} q_i^{k_i} \prod_{\substack{q_i \mid d \\ q_i \equiv 5 \pmod 8}} q_i^{k_i} \prod_{\substack{q_i \mid d \\ q_i \equiv 7 \pmod 8}} q_i^{k_i},$$

$$\equiv \prod_{\substack{q_i \mid d \\ q_i \equiv 3 \pmod 8}} (3)^{k_i} \prod_{\substack{q_i \mid d \\ q_i \equiv 5 \pmod 8}} (-3)^{k_i} \prod_{\substack{q_i \mid d \\ q_i \equiv 7 \pmod 8}} (-1)^{k_i} \pmod 8,$$

$$\equiv \prod_{\substack{q_i \mid d \\ q_i \equiv 3,5 \pmod 8}} (3)^{k_i} \prod_{\substack{q_i \mid d \\ q_i \equiv 5,7 \pmod 8}} (-1)^{k_i} \pmod 8.$$

Si $n \equiv 1$ ou $5 \pmod 8$,alors

$$c = 3 \text{ et } d = 8j + 3 \equiv 3 \pmod 8,$$

alors

$$\sum_{\substack{q_i \mid d \\ q_i \equiv 3,5 \pmod 8}} k_i \equiv 1 \pmod 2,$$

et

$$\sum_{\substack{q_i \mid d \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2,$$

Si $n \equiv 3 \pmod 8$,alors

$$c = 1 \text{ et } d = 8j + 1 \equiv 1 \pmod 8,$$

et par suite

$$\sum_{\substack{q_i \mid d \\ q_i \equiv 3,5 \pmod 8}} k_i \equiv 0 \pmod 2,$$

et

$$\sum_{\substack{q_i \mid d \\ q_i \equiv 5,7 \pmod 8}} k_i \equiv 0 \pmod 2,$$

donc $-d$ est un residue quadratique modulo $2p = dn - 1$

d'ou on peut écrire n comme somme de trois nombres carrés. ■

Théorème 4 (Gauss) *On trouve $n, l, k \in \mathbb{N}$, alors n est une somme de trois nombres carrés si et seulement si*

$$n \neq 4^k (8l + 7).$$

Preuve. On a

$$x^2 \equiv 0, 1 \text{ ou } 4 \pmod 8,$$

pour chaque nombre entier x, il suit qu'une somme de trois nombres carrés peut jamais être congruent à 7 modulo 8.

Si le nombre entier $4m$ est une somme de trois nombres carrés, alors la existent des nombres entiers x_1, x_2, x_3 tels que

$$4m = x_1^2 + x_2^2 + x_3^2,$$

c'est possible si seulement si x_1, x_2, x_3 sont pairs, et alors

$$m = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2,$$

alors $4^k m$ est un somme de trois nombres carrés si et seulement si m est un somme de trois nombres carrés

Ceci montre qu'aucun nombre entier de la forme $4^k(8l + 7)$ ne peut être une somme de trois nombres carrés

Chaque nombre entier positif n peut être écrit uniquement sous la forme

$$n = 4^k m,$$

avec

$$m \equiv 2 \pmod 4 \ \text{ ou } m \equiv 1, 3, 5 \text{ ou } 7 \pmod 8,$$

d'après lemme (1) et (2) n est un somme de trois nombres carrés sauf

$$m \equiv 7 \pmod 8,$$

■

Chapitre 2

Formules des sommes

Dans ce chapitre, nous allons présenter quatre cas des formules des sommes de quatre nombres polygonaux , pour ce là, dans chaque cas on va commencer tout d'abord par le théorème, puis quelques lemmes utiles pour la démonstration de ce dernier, et terminons par quelques résultats.

2.1 Première formule

Théorème 5 (1) *Soient* $m \in \mathbb{Z}^+$ *et* x_1, x_2, x_3 *et* $x_4 \in \mathbb{N}$. *tels que* $4 \mid m$,

i) Tout entier $N \geq 28m^3$ *peut être écrit sous la forme suivante:*

$$P_{m+2}(x_1) + P_{m+2}(x_2) + P_{m+2}(x_3) + P_{m+2}(x_4).$$

ii) Il existe une infinité des nombres entiers ne peut être écrit comme

$$P_{m+4}(x_1) + P_{m+4}(x_2) + P_{m+4}(x_3) + P_{m+4}(x_4) \quad \textit{pour } m \neq 4.$$

Pour démontrer ce théorème on a besoin des lemmes suivants

2.1.1 Lemme 1

La longueur de l'intervalle

$$I = \left[\frac{1}{2} + \sqrt{\frac{6N}{m} - 3}, \frac{2}{3} + \sqrt{\frac{8N}{m}}\right], \tag{2.1}$$

est supérieur à lm, pour tout l, m et N dans $\mathbb{Z}^+$, avec $N \geq 7l^2m^3$.

Preuve. Soit L la longueur de l'intrvalle I, et on pose que

$$x = \frac{N}{m},$$

on a alors

$$x \geq 7l^2m^2$$

et

$$\begin{aligned} L &= \frac{2}{3} + \sqrt{\frac{8N}{m}} - \frac{1}{2} + \sqrt{\frac{6N}{m} - 3} \\ &= \sqrt{8x} - \sqrt{6x-3} + \frac{1}{6}. \end{aligned}$$

Soit

$$l_0 = lm - \frac{1}{6},$$

on a

$$\begin{aligned} L > lm &\iff \sqrt{8x} - \sqrt{6x-3} \geq l_0 \\ &\iff \sqrt{8x} > \sqrt{6x-3} + l_0 \\ &\iff \sqrt{8x} > 6x - 3 + l_0^2 + 2l_0\sqrt{6x-3} \\ &\iff 2x + 3 - l_0^2 > 2l_0\sqrt{6x-3}, \end{aligned}$$

donc

$$L > lm \iff 14x + 21 - 7l_0^2 > 14l_0\sqrt{6x-3} \ ,$$

comme

$$x \geq 7l_0^2,$$

donc

$$\begin{aligned} L > lm &\iff 13x + 21 - 14l_0\sqrt{6x-3} \\ &= 7x + 18 + \left(7l_0 - \sqrt{6x-3}\right)^2 - 7\left(7l_0\right)^2 \\ &= 18 + \left(7l_0 - \sqrt{6x-3}\right)^2 > 0. \end{aligned}$$

■

2.1.2 Lemme 2

Soient a, b, m et *$N \in \mathbb{Z}^+$tels que $m \geq 3$, et*

$$N = \frac{m}{2}(a-b) + b \geq \frac{2}{3}m,$$

on *suppose que $b \in I$,*

où

$$I=\left[\frac{1}{2}+\sqrt{\frac{6N}{m}-3},\frac{2}{3}+\sqrt{\frac{8N}{m}}\right],$$

alors

$$b^2<4a,\quad \text{et}\quad 3a<b^2+2b+4.$$

Preuve. 1) Pour montrer que $b^2<4a$ il suffit de prouver que

$$b^2-4a<0.$$

On a:

$$b^2-4a=b^2-4\left(1-\frac{2}{m}\right)b-\frac{8N}{m},$$

c'est une formule quadratique

$$\begin{aligned}
\Delta &= 4^2\left(1-\frac{2}{m}\right)^2+32\frac{N}{m}>0\\
b_1 &= 2\left(1-\frac{2}{m}\right)+2\sqrt{\left(1-\frac{2}{m}\right)^2+\frac{2N}{m}}\\
b_2 &= 2\left(1-\frac{2}{m}\right)-2\sqrt{\left(1-\frac{2}{m}\right)^2+\frac{2N}{m}}.
\end{aligned}$$

alors

$$b^2-4a<0,$$

si

$$0<b<2\left(1-\frac{2}{m}\right)+2\sqrt{\left(1-\frac{2}{m}\right)^2+\frac{2N}{m}},$$

et comme $b\in I$ alors on a

$$\begin{aligned}
0<b &< \frac{2}{3}+\sqrt{\frac{8N}{m}}\\
&\leq 2\left(1-\frac{2}{m}\right)+\sqrt{\frac{8N}{m}}\\
&\leq 2\left(1-\frac{2}{m}\right)+2\left(1-\frac{2}{m}\right)^2+\frac{2N}{m},
\end{aligned}$$

donc

$$I\subset[b_1,b_2],$$

alors

$$\forall b\in I\Longrightarrow b^2-4a<0.$$

2) Pour montrer que $3a<b^2+2b+4$ il suffit de prouver que

$$b^2+2b+4-3a>0.$$

On étudie la formule quadratique

$$b^2 + 2b + 4 - 3a = b^2 - \left(1 - \frac{6}{m}\right) b - \frac{6N}{m} + 4,$$

$$\begin{aligned}
\Delta &= \left(1 - \frac{6}{m}\right)^2 + 4\left(\frac{6N}{m} - 4\right) > 0 \\
b_1 &= \left(\tfrac{1}{2} - \frac{3}{m}\right) + 2\sqrt{\left(\tfrac{1}{2} - \frac{3}{m}\right)^2 + \frac{6N}{m} - 4} \\
b_2 &= \left(\tfrac{1}{2} - \frac{3}{m}\right) - 2\sqrt{\left(\tfrac{1}{2} - \frac{3}{m}\right)^2 + \frac{6N}{m} - 4},
\end{aligned}$$

alors

$$b^2 + 2b + 4 - 3a > 0,$$

si

$$b > \left(\frac{1}{2} - \frac{3}{m}\right) + 2\sqrt{\left(\frac{1}{2} - \frac{3}{m}\right)^2 + \frac{6N}{m} - 4}.$$

comme $b \in I$, alors

$$\begin{aligned}
b &> \frac{1}{2} + \sqrt{\frac{6N}{m} - 3} \\
&\geq \left(\frac{1}{2} - \frac{3}{m}\right) + \sqrt{\frac{6N}{m} - 3} \\
&\geq \left(\frac{1}{2} - \frac{3}{m}\right) + 2\sqrt{\left(\tfrac{1}{2} - \frac{3}{m}\right)^2 + \frac{6N}{m} - 4},
\end{aligned}$$

donc si

$$b \in I \Longleftrightarrow b^2 + 2b + 4 - 3a > 0,$$

■

2.1.3 Lemme 3

soient a, b et $c \in \mathbb{N}$ *et soient* $x, y, z \in \mathbb{R}$ *alors l'inégalité suivantes est toujour vérifié*

$$(ax + by + cz)^2 \leq (a + b + c)\left(ax^2 + by^2 + cz^2\right).$$

Preuve. D'aprés l'inégalité de cauchy schwarz

$$\begin{aligned}
(ax + by + cz)^2 &= \left(\sqrt{a}\sqrt{a}x + \sqrt{b}\sqrt{b}y + \sqrt{c}\sqrt{c}z\right)^2 \\
&\leq (a + b + c)\left(ax^2 + by^2 + cz^2\right).
\end{aligned}$$

■

2.1.4 Lemme 4

soit a et b deux entiers tels que

$$b^2 < 4a, \text{et } 3a < b^2 + 2b + 4.$$

Supposons que $2 \nmid ab$, alors il existe $s, t, u, v \in \mathbb{N}$ tels que:

$$\begin{aligned} a &= s^2 + t^2 + u^2 + v^2 \\ b &= s + t + u + v. \end{aligned}$$

Preuve. on a

$$4a - b^2 \equiv 3 \pmod 8,$$

car

$$\begin{aligned} 4a - b^2 &= 4(2n+1) - (2m+1)^2 \\ &= 8n - 4a(a+1) + 3 \\ &= 8l + 3 \\ &\equiv 3 \pmod 8. \end{aligned}$$

D'après le théorème 4:

$$4a - b^2 = x^2 + y^2 + z^2 \setminus \; 2 \nmid xyz,$$

alors

$$a = \frac{b^2 + x^2 + y^2 \pm z^2}{4}.$$

On choisit le signe de $\pm z$ pour:

$$b^2 + x^2 + y^2 \pm z^2 \equiv 0 \pmod 4.$$

On définit les nombres $s, t, u, v \in \mathbb{Z}$ tels que:

$$\begin{aligned} s &= \frac{b + x + y \pm z}{4} \\ t &= \frac{b + x}{2} - s = \frac{b + x - y \pm z}{4} \\ u &= \frac{b + y}{2} - s = \frac{b - x + y \pm z}{4} \\ v &= \frac{b \pm z}{2} - s = \frac{b - x - y \pm z}{4}. \end{aligned}$$

On remarque que

$$s + t + u + v = b,$$

et on a

$$\begin{aligned} s^2+t^2+u^2+v^2 &= 2\left(\frac{s+t}{2}\right)^2+2\left(\frac{s+t}{2}\right)^2+2\left(\frac{s+t}{2}\right)^2+2\left(\frac{s+t}{2}\right)^2 \\ &= 2\left(\frac{s+t}{4}\right)^2+2\left(\frac{s+t}{4}\right)^2+2\left(\frac{s+t}{4}\right)^2+2\left(\frac{s+t}{4}\right)^2 \\ &= \frac{b^2+x^2+y^2\pm z^2}{4}=a. \end{aligned}$$

il reste de montrer que $s, t, u, v \in \mathbb{N}$.

On a

$$s \geq t \geq u \geq v = \frac{b-x-y \pm z}{4},$$

et on a d'après lemme (3)

$$\begin{aligned} x+y+z &\leq \sqrt{3\left(4a-b^2\right)} \\ &\leq \sqrt{12a-3b^2} \\ &< \sqrt{b^2+8b+16} \\ &= b+4, \end{aligned}$$

donc

$$\begin{aligned} x+y+z<b+4 &\Longrightarrow \frac{b-x-y \pm z}{4} > -1 \\ &\Longrightarrow v \geq 0. \end{aligned}$$

d'ou $s, t, u, v \in \mathbb{N}$. ■

2.1.5 Lemme 5

Pour tout $n \in \mathbb{N}$, on a

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d,$$

tels que

$$r_4(n) = \left|\left\{(w,x,y,z) \in \mathbb{Z}^4 : w^2+x^2+y^2+z^2=n\right\}\right|.$$

2.1.6 Démonstration du théorème (1)

i) Soit

$$I_1 = \left[\frac{1}{2}+\sqrt{\frac{6N}{m}-3}, \frac{2}{3}+\sqrt{\frac{8N}{m}}\right],$$

comme

$$N \geq 28m^3 \geq 7 \times 2^2 \times m^2,$$

alors d'après lemme(1), la longueur de I_1 est supérieur à $2m$ donc il existe un nombre entier appartenant à I_1soit

$$b_1 \in \left\{ \left[\frac{1}{2} + \sqrt{\frac{6N}{m} - 3} \right] + r : r = 0...m-1 \right\},$$

alors

$$\begin{aligned} b_2 = b_1 + m \quad & \leq \frac{1}{2} + \sqrt{\frac{6N}{m} - 3} + 2m - 1 \\ & \leq \frac{1}{2} + \sqrt{\frac{6N}{m} - 3} + 2m \\ & < \frac{2}{3}\sqrt{\frac{6N}{m}}, \end{aligned}$$

donc

$$[b_1, b_2] \subset I_1.$$

Soit

$$b \in [b_1, b_2]$$

tels que

$$N \equiv b \pmod{m}$$

alors

$$N = km + b$$

pour tout $k \in \mathbb{Z}^+$, soit $a \in \mathbb{Z}^+$ tels que

$$k = \frac{a-b}{2}, \text{ avec } a > b$$

donc

$$N = \frac{m}{2}(a-b) + b,$$

$$\begin{aligned} a \quad & = 2\left(\frac{N-b}{m}\right) + b \\ & = \left(1 - \frac{2}{m}\right) b + \frac{2N}{m}, \end{aligned}$$

comme b est impair alors a est impair

donc d'après le lemme(2) on a

$$b^2 < 4a,$$

et

$$3a < b^2 + 2b + 4.$$

et d'après le lemme (4) , il existe $s, t, u, v \in \mathbb{N}$ telle que

$$\begin{aligned} a &= s^2 + t^2 + u^2 + v^2 \\ b &= s + t + u + v. \end{aligned}$$

donc

$$\begin{aligned} N &= \frac{m}{2}(a-b) + b, \\ &= \frac{m}{2}\left(s^2 + t^2 + u^2 + v^2 - s - t - u - v\right) + s + t + u + v, \\ &= \frac{m}{2}\left(s^2 - s\right) + s\frac{m}{2}\left(t^2 - t\right) + t + \frac{m}{2}\left(u^2 - u\right) + u \\ &+ \frac{m}{2}\left(v^2 - v\right) + v, \\ &= \frac{ms^2 - (m-2)s}{2} + \frac{mt^2 - (m-2)t}{2} + \frac{mu^2 - (m-2)u}{2}, \\ &+ \frac{mv^2 - (m-2)v}{2}, \\ &= P_{m+2}(s) + P_{m+2}(t) + P_{m+2}(u) + P_{m+2}(v). \end{aligned}$$

ii) On pose $m = 4l$ avec $l \in \mathbb{Z}^+$, soit φ fonction indicatrice d'Euler, il suffit de prouver que pour tout nombres entiers positives

$$4l^2 \frac{4^{k\varphi(2l+1)} - 1}{2l+1} \quad \backslash\ k = 1, 2, 3...$$

ne peut être écrit comme

$$P_{m+4}(x_1) + P_{m+4}(x_2) + P_{m+4}(x_3) + P_{m+4}(x_4).$$

Supposons qu'il existe $n \in \mathbb{Z}^+$ avec

$$\varphi(2l+1) \mid n,$$

alors

$$k\varphi(2l+1) = n,$$

on suppose qu'il existe w, x, y et $z \in \mathbb{N}$ tels que

$$\begin{aligned} 4l^2 \frac{4^n - 1}{2l+1} &= P_{m+4}(x_1) + P_{m+4}(x_2) + P_{m+4}(x_3) + P_{m+4}(x_4), \\ &= \frac{(m+2)w^2 - mw}{2} + \frac{(m+2)x^2 - mx}{2} + \frac{(m+2)y^2 - my}{2} \\ &+ \frac{(m+2)z^2 - mz}{2}, \\ &= \frac{(m+2)\left(w^2 - w\right)}{2} + w + \frac{(m+2)\left(x^2 - x\right)}{2} + x \\ &+ \frac{(m+2)\left(y^2 - y\right)}{2} + y + \frac{(m+2)\left(z^2 - z\right)}{2} + z, \end{aligned}$$

comme $4l = m$ alors

$$4l^2 \frac{4^n - 1}{2l+1} = \frac{4l+2}{2} \left(w^2 + x^2 + y^2 + z^2 - w - x - y - z\right) + w + x + y + z,$$

alors

$$\begin{aligned} 4^{n+1} l^2 &= (4l+2) \left(w^2 + x^2 + y^2 + z^2\right) - (2l+1)(w + x + y + z), \\ &= ((2l+1) w - l)^2 + ((2l+1) x - l)^2, \\ &+ ((2l+1) y - l)^2 + ((2l+1) z - l)^2, \end{aligned}$$

comme

$$r_4(4^{n+1} l^2) = r_4(4l^2),$$

d'aprés le lemme (5), il existe $w_0, x_0, y_0, z_0 \in \mathbb{Z}$ tels que

$$w_0^2 + x_0^2 + y_0^2 + z_0^2 = 4l^2,$$

donc

$$\begin{aligned} 4^{n+1} l^2 &= 4^n \left(w_0^2 + x_0^2 + y_0^2 + z_0^2\right) \\ &= (2^n w_0)^2 + (2^n x_0)^2 + (2^n y_0)^2 + (2^n z_0)^2, \end{aligned}$$

alors

$$(2l+1) w - l = 2^n w_0,$$

$$(2l+1) x - l = 2^n x_0,$$

$$(2l+1) y - l = 2^n y_0,$$

$$(2l+1) z - l = 2^n z_0,$$

d'aprés théorème 1 on a

$$2^{\varphi(2l+1)} = 2^n \equiv 1 (\operatorname{mod} 2l+1),$$

et on a

$$2^n w_0 = -l \operatorname{mod} (2l+1),$$

$$2^n x_0 = -l \operatorname{mod} (2l+1),$$

$$2^n y_0 = -l \operatorname{mod} (2l+1),$$

$$2^n z_0 = -l \operatorname{mod} (2l+1),$$

donc

$$w_0 \equiv x_0 \equiv y_0 \equiv z_0 \equiv -l \bmod (2l+1),$$

comme

$$w_0^2 + x_0^2 + y_0^2 + z_0^2 = 4l^2,$$

alors

$$w_0 = x_0 = y_0 = z_0 = -l,$$

on a

$$(2l+1)w = 2^n w_0 + l = l(1-2^n) < 0.$$

C'est une contradiction car $w \in \mathbb{N}$, donc il existe une infinité des nombres entiers qui ne peut pas être écrit sous la forme

$$P_{m+4}(x_1) + P_{m+4}(x_2) + P_{m+4}(x_3) + P_{m+4}(x_4).$$

2.1.7 Corollaire 1

On a

$$\begin{aligned}&\{P_6(x_1) + P_6(x_2) + P_6(x_3) + P_6(x_4), \quad x_1, x_2, x_3, x_4 \in \mathbb{N}\}\\&= \mathbb{N} \backslash \{5, 10, 11, 20, 25, 26, 38, 39, 54, 65, 70, 114, 130\},\end{aligned}$$

et alors, tout $n \in \mathbb{N}$ peut être écrit comme une somme de un nomber triangulair et trois nombers hexagonaux

aussi $\forall n > 2146$ peut être écrit comme une somme de quatre nombres decagonaux et on a

$$\begin{aligned}&\{P_{10}(x_1) + P_{10}(x_2) + P_{10}(x_3) + P_{10}(x_4), \quad x_1, x_2, x_3, x_4 \in \mathbb{N}\}\\&= \mathbb{N} \backslash \{5, 6, 26\}.\end{aligned}$$

preuve. D'aprés théorème 5 (1), tout les nombers entiers $n > 28 \times 4^3$ peut être ecrit comme somme de qautre nombers henagonaux, avec $m = 4.11$

On utilise l'algorithme $[A]$, on peut vérifier que

$$5, 10, 11, 20, 25, 26, 38, 39, 54, 65, 70, 114, 130,$$

sont les seuls nombres entiers positives inférieurs à 28×4^3 que ne peut étre écrit comme une sommes de qautre nombers henagonaux, et on a

$$\begin{aligned}
5 &= P_3(2) + P_6(3) + P_6(1) + P_6(0),\\
10 &= P_3(4) + P_6(0) + P_6(0) + P_6(0),\\
11 &= P_3(4) + P_6(1) + P_6(0) + P_6(0),\\
20 &= P_3(2) + P_6(3) + P_6(1) + P_6(1),\\
25 &= P_3(4) + P_6(3) + P_6(0) + P_6(0),\\
26 &= P_3(4) + P_6(3) + P_6(1) + P_6(0),\\
38 &= P_3(8) + P_6(1) + P_6(1) + P_6(1),\\
65 &= P_3(8) + P_6(4) + P_6(1) + P_6(0),\\
70 &= P_3(10) + P_6(3) + P_6(0) + P_6(0,\\
114 &= P_3(5) + P_6(7) + P_6(0) + P_6(0),\\
130 &= P_3(5) + P_6(7) + P_6(3) + P_6(1).
\end{aligned}$$

Aussi on a d'apres Théorème 5 (1) , tout $n = 2147, ..., 2858^3 - 1$ est une somme de quatre nombres decagonaux et $5, 6$ et 26 sont les seuls nombres naturels inférieure à 2147 qui ne peut étre pas écrit comme somme de quatre nombres decagonaux (on uitlise la méme algorithme $[A]$ pour vérifier ce résultat). ■

2.2 Deuxième formule

Théorème 6 (2) *On trouve $m \geq 3$, $m \in \mathbb{Z}$.*

i) Supposons que $2 \nmid m$ ou $4 \mid m$, alors $\forall N \geq 1628m^3$, on peut écrire N sous la forme

$$P_{m+1}(x_1) + P_{m+2}(x_2) + 2P_{m+2}(x_3) + 2P_{m+2}(x_4),$$

pour tout $x_1, x_2, x_3, x_4 \in \mathbb{N}$.

ii) Si $m \equiv 2 (\mathrm{mod}\, 4)$,alors il existe une infinité des nombres entiers ne peut être écrit sous la forme

$$P_{m+1}(x_1) + P_{m+2}(x_2) + 2P_{m+2}(x_3) + 2P_{m+2}(x_4),$$

pour x_1, x_2, x_3 et $x_4 \in \mathbb{N}$.

Voici quelques lemmes utiles pour la démonstration du théorème précedent

2.2.1 Lemme 6

Soit $l, m, N \in \mathbb{Z}^+$, tels que

$$N \geq 11lm^2(lm+1),$$

alors la longueur de l'intervalle

$$I_2 = \left[\frac{3}{2} + \sqrt{\frac{10N}{m} - 3}, 1 + \sqrt{\frac{12N}{m}}\right],$$

est supérieur à $l\ m$.

Preuve. Soit L_2 la longueur de l'intervalle I_2, et on pose

$$x = \frac{N}{m},$$

on a alors

$$x \geq 11lm(lm+1),$$

et

$$L_2 = \sqrt{12x} - \sqrt{10x-3} - \frac{1}{2},$$

soit

$$l_0 = lm + \frac{1}{2},$$

alors

$$\begin{aligned} L_2 > lm &\iff \sqrt{12x} - \sqrt{10x-3} \geq l_0 \\ &\iff \sqrt{12x} > \sqrt{10x-3} + l_0 \\ &\iff 12x > 10x - 3 + l_0^2 + 2l_0\sqrt{10x-3} \\ &\iff 2x + 3 - l_0^2 < 2l_0\sqrt{10x-3} \\ &\iff 4x(x - 11l_0^2 + 3) + (l_0^2 - 3)^2 + 12l_0^2 > 0, \end{aligned}$$

comme

$$\begin{aligned} x &\geq 11lm(lm+1) \\ &> 11^2m^2 + 11lm + \tfrac{11}{4} - 3 \\ &= 11l_0^2 - 3, \end{aligned}$$

donc

$$L_2 > lm.$$

■

2.2.2 Lemme 7

Soient $a, b, m, N \in \mathbb{Z}$, tels que $m \geq 3$ et

$$N = \frac{m}{2}(a-b) + b \geq \frac{3}{5}m,$$

I_2 l'intervalle donnée sur le lemme(6), alors

$$b^2 < 6a \tag{2.2}$$

et

$$5a \; < b^2 + 2b + 6. \tag{2.3}$$

Preuve.

Pour montrer (2.2) il suffit de démontrer que:

$$b^2 - 6a < 0,$$

on a

$$a = (1 - \frac{2}{m})b + \frac{2N}{m},$$

alors

$$b^2 - 6a = b^2 - 6(1 - \frac{2}{m})b - \frac{12N}{m},$$

c'est est une fourmule quadratique:

$$\triangle = 6^2(1 - \frac{2}{m})^2 + \frac{48N}{m} > 0,$$

et les racines sont:

$$b_1 = 3(1 - \frac{2}{m}) + \sqrt{9(1 - \frac{2}{m})^2 + \frac{12N}{m}},$$

$$b_2 = 3(1 - \frac{2}{m}) - \sqrt{9(1 - \frac{2}{m})^2 + \frac{12N}{m}},$$

alors

$$b^2 - 6a < 0,$$

si

$$0 < b < 3(1 - \frac{2}{m}) + \sqrt{9(1 - \frac{2}{m})^2 + \frac{12N}{m}},$$

et comme $b \in I_2$ alors:

$$\begin{aligned} 0 < b \; &< 1 + \sqrt{\frac{12N}{m}} \\ &\leq 3(1 - \frac{2}{m}) + \frac{12N}{m} \\ &\leq 3(1 - \frac{2}{m}) + \sqrt{9(1 - \frac{2}{m})^2 + \frac{12N}{m}}. \end{aligned}$$

Donc

$$I_2 \subset [b_1, b_2]$$

alors

$$\forall b \in I \Longrightarrow b^2 - 6a > 0$$

Pour montrer (2.3) il suffit de prouver que:

$$b^2 + b + 6 - 5a > 0.$$

On étude le signe de la formule quadratique

$$b^2 + 2b - 6 - 5a = b^2 - (3 - \frac{10}{m})b + (6 - \frac{10N}{m}).$$

$$\triangle = (3 - \frac{10}{m})^2 - (6 - \frac{10N}{m}) > 0,$$

comme

$$(6 - \frac{10N}{m}) < 0$$

alors

$$b_1 = (\frac{3}{2} - \frac{5}{m}) - \sqrt{(\frac{3}{2} - \frac{5}{m})^2 + \frac{10N}{m} - 6},$$
$$b_2 = (\frac{3}{2} - \frac{5}{m}) + \sqrt{(\frac{3}{2} - \frac{5}{m})^2 + \frac{10N}{m} - 6}.$$

Donc:

$$b^2 + 2b - 6 - 5a > 0.$$

si $b \in \mathbb{R} \setminus \{b_1, b_2\}$ comme $b \in I_2$ alors:

$$\begin{aligned} b &\geq \tfrac{3}{2} + \sqrt{\tfrac{10N}{m} - 3} \\ &\geq (\tfrac{3}{2} - \frac{5}{m}) + \sqrt{(\tfrac{3}{2} - \frac{5}{m})^2 + \frac{10N}{m} - 6} \\ &= b_2, \end{aligned}$$

donc

$$b \in I_2 \Longrightarrow b^2 + 2b - 6 - 5a > 0,$$

■

2.2.3 Lemme 8

Soient $a, b \in \mathbb{Z}^+$ tels que $a \equiv b (\bmod 2)$, vérifient (2.2) et (2.3),

supposons que

$$(2 \mid a \text{ ou } 4 \parallel a) \text{ et } (3 \mid a \text{ ou } 3 \mid b),$$

alors il éxiste s, t, u et $v \in \mathbb{N}$ tels que

$$a = s^2 + t^2 + 2u^2 + 2v^2 \text{ et } b = s + t + 2u + 2v.$$

Preuve. Si $n \in \mathbb{N}$, tels que $n \neq 4^k(8l + 7)$, pour $k, l \in \mathbb{N}$.

D'après le théorème 4 (Gauss), il éxiste x, u et $v \in \mathbb{Z}$, avec $u \equiv v(\bmod 2)$, tels que

$$\begin{aligned} n &= x^2 + y^2 + z^2 \\ &= x^2 + 2(\frac{u-v}{2})^2 + 2(\frac{u+v}{2})^2. \end{aligned}$$

nous prétendons que il existe x, y et $z \in \mathbb{Z}$

tels que

$$6a - b^2 = x^2 + 2y^2 + 2z^2$$

alors

$$\begin{aligned} s &= \frac{b + x + 2y + 2z}{6}, \\ t &= \frac{b - x - 2y + 2z}{6}, \\ u &= \frac{b - x + y - z}{6} = t + \frac{y - z}{2}, \\ v &= \frac{b + x - y - z}{6} = s - \frac{y + z}{2}. \end{aligned} \tag{2.4}$$

sont des entiers ■

1. **Lemme 3** ***Preuve.***

cas 1. $3 \nmid b$

Si

$$a \equiv b \equiv 1 \,(\bmod 2)\,,$$

alors

$$6a - b^2 \equiv 1(\bmod 4)$$

quand $4 \parallel a$ *et* $2 \mid b$

on a

$$6a - b^2 \equiv 4, 8(\bmod 16)$$

ainsi

$$6a - b^2 = x^2 + 2y^2 + 2z^2$$

il est clair que

$$x \equiv b \,(\bmod 2) \;\; \textit{et } y \equiv z \,(\bmod 2)$$

alors

$$x^2 + 2y^2 + 2z^2 \equiv 6a - b^2 \equiv 2 \pmod 3.$$

Comme

$$x^2 \not\equiv 2 \pmod 3$$

on a $3 \nmid y$ *ou* $3 \nmid z$

Sans perte de généralité, on peut supposer que $3 \nmid z$ *et* $z \equiv b \pmod 3$

$($*si* $z \equiv b \pmod 3$ *alors* $-z \equiv b \pmod 3))$

Comme

$$x^2 - y^2 \equiv x^2 + 2y^2 \equiv 0 \pmod 3)$$

sans perte de généralité, on peut supposer que $x \equiv y \pmod 3)$

donc s, t, u *et* $v \in \mathbb{Z}$

cas 2. $3 \mid a$ *et* $3 \mid b$

On pose

$$a = 3a_0 \text{ et } b = 3b_0,$$

pour tout $a_0, b_0 \in \mathbb{Z}$.

Si

$$a \equiv b \equiv 1 (\text{mod}\, 2),$$

alors

$$2a_0 - b_0^2 \equiv 1 (\text{mod}\, 4),$$

quand

$$4 \parallel a \text{ et } 2 \mid b.$$

On a

$$2a_0 - b_0^2 \equiv 4, 8 (\text{mod}\, 16),$$

aussi

$$2a_0 - b_0^2 = x_0^2 + 2y_0^2 + 2z_0^2,$$

pour tout x_0, y_0 *et* $z_0 \in \mathbb{Z}$, *et par suite*

$$x_0 \equiv b_0 (\text{mod}\, 2) \text{ et } y_0 \equiv z_0 (\text{mod}\, 2),$$

tels que

$$a_0 \equiv b_0 (\text{mod}\, 2),$$

on a

$$x = 3x_0 \ et \ z = 3z_0 \ et \ y = 3y_0.$$

alors

$$6a - b^2 = 9(2a_0 - b_0^2) = x^2 + 2y^2 + 2z^2,$$

et tous les nombres dans (2.4) *sont des entiers.*

d'ou $s, t, u, v \in \mathbb{Z}$ *pour les deux cas.*

Il reste de montrer que s, t, u *et* $v \in \mathbb{N}$ *(c'est-à-dire* $s, t, u, v \geq 0$*)*

On a

$$x^2 + 2y^2 + 2z^2 = 6a - b^2,$$

et $s, t, u, v \in \mathbb{Z}$.

On observe que:

$$s + t + 2(u + v) = \frac{b + 2z}{3} + 2\frac{b - z}{3} = b,$$

et

$$\begin{aligned} s^2 + t^2 + 2u^2 + 2v^2 &= 2\left(\frac{s+t}{2}\right)^2 + 2\left(\frac{s-t}{2}\right) + (u + v)^2 + (u - v^2), \\ &= 2\left(\frac{b+2z}{6}\right)^2 + 2\left(\frac{x+2y}{6}\right) + (\frac{b-z}{3})^2 + (\frac{x-y}{3}), \\ &= \frac{b^2 + x^2 + 2y^2 + 2z^2}{6} = a. \end{aligned}$$

D'aprés le lemme (3) *et le lemme* (7) *on a*

$$\begin{aligned} (|x| + 2|y| + 2|z|)^2 &\leq 5(x^2 + 2y^2 + 2z^2) \\ &= 5(6a - b^2) \\ &< (b + 6)^2, \end{aligned}$$

et on a

$$b - |x| - 2|y| - 2|z| > -6,$$

donc

$$s, t, u, v \geq \frac{b - |x| - 2|y| - 2|z|}{6} > -1$$

d'ou $s, t, u, v \in \mathbb{N}$, $\blacksquare$

2.2.4 Démonstration du théorème (2)

i) Soit

$$I_2 = \left[\frac{3}{2} + \sqrt{\frac{10N}{m}} - 3, 1 + \sqrt{\frac{12N}{m}}\right] = [\alpha, \beta],$$

est l'intervalle qui donnée sur le lemme (6).

Comme

$$N \geq 1628m^3 = (12 + \frac{1}{3})m \times 132m^2$$

$$\geq 11m^2 \times 12(12m+1).$$

D'après le lemme(6), la longueur de I_2 est supérieur à $12m$.

On distinguons deux cas pour construire les nombres entiers

$$b \in I_2 \text{ et } a \equiv b (\operatorname{mod} 2),$$

pour

$$N = \frac{m}{2}(a-b) + b$$

et $2 \nmid a$ ou $4 \parallel a$, et $3 \mid a$ ou $3 \nmid b$.

cas 1 $3 \nmid m$ ou $3 \nmid N$.

On pose

$$b_0 \equiv N (\operatorname{mod} m),$$

tels que

$$b_0 \in \left\{ \left[\frac{3}{2} + \sqrt{\frac{10N}{m} - 3} \right] + r : r = 0, \ldots, m-1 \right\},$$

Soit

$$b_j = b_0 + jm$$

pour $j = 1, \ldots, 4$

on a

$$[\alpha] + 8m - 1 < \alpha + 8m < \beta.$$

Soit $b_i \in I_2$ pour tout $i = 0, \ldots, 7$.

Si $2 \nmid m$, alors on choisit $i \in \{0, 1\}$ pour b_i est impaire , alors $4 \mid m$,

nous pouvons choisit $i \in \{0, 1, 2, 3\}$

tels que

$$a_i := \frac{2}{m}(N - b_i) + b_i \equiv 4 (\operatorname{mod} 8),$$

on a

$$a_i - a_0 = -2i + im$$

$$= 2i(\frac{m}{2} - 1),$$

pour $\frac{m}{2} - 1$ est impaire.

Si $3 \mid m$ et $3 \nmid N$, alors

$$b = b_i \equiv N \not\equiv o(\bmod 3),$$

tels que $3 \nmid m$, on choisit $j \in \{i, i+4\}$

pour

$$b = b_j \not\equiv 0(\bmod 3),$$

et on note

$$a_{i+4} - a_i = 4m - 8 \equiv \begin{cases} 0(\bmod 2) \text{ si } 2 \nmid m \\ \\ 0(\bmod 8) \text{ si } 4 \mid m. \end{cases}$$

Comme

$$N \equiv b(\bmod m),$$

on remarque que

$$a = \frac{2(N-b)}{m+b},$$

est un nombre entier, pour

$$a \equiv b(\bmod 2).$$

Par notre choix, $2 \nmid b$ si

$$2 \nmid m \text{ et } a \equiv 4(\bmod 8).$$

Si $4 \mid m$ on note alors que $3 \nmid b$

cas2 $m \equiv N \equiv 0 \,(\bmod 3)\,,$

On choisit

$$b_0 \in \{[\alpha] + r : r = 0, 1, ..., 3m - 1\}\,,$$

si$2 \nmid m$, alors on choisit $b \in \{b_0, b_0 + 3m\}$ pour b est impair,

et par Conséquence

$$a = \frac{2}{m}\,(N-b) + b \equiv b \equiv 1\,(\bmod 2)\,.$$

Alors $4 \mid m$, on peut choisit

$$b \in \{b_0 + 3jm : j = 0, 1, 2, 3\}$$

tels que

$$a = \frac{2}{m}(N - b) + b \equiv 4 \pmod 8,$$

pour

$$\frac{2}{m}(N - b_0 - 3\sin) + b_0 + 3jm - \left(\frac{2}{m}(N - b_0) + b_0\right)$$

$$= 6j\left(\frac{m}{2} - 1\right),$$

avec $\frac{m}{2} - 1$ est impair.

On note que

$$\alpha \leq b_0 \leq b_0 + 9m \leq [\alpha] + 3m - 1 + 9m < \beta,$$

et par conséquence $b \in I_2$.

On obeserve que

$$a \equiv b \equiv N \equiv 0 \pmod 3.$$

Maintenant nous avons construit les nombres entiers positive $b \in I_2$

et

$$a \equiv b \pmod 2$$

avec

$$N = \frac{m}{2}(a - b) + b,$$

tels que

$$2 \nmid a \text{ ou } 4 \parallel a, \text{et } 3 \mid a \text{ ou } 3 \nmid b$$

donc d'aprés le lemme (7) on a

$$b^2 < 6a \text{ et } 5a < b^2 + 2b + b,$$

et d'aprés le lemme (8), alors il existe $s, t, u, v \in \mathbb{N}$ tels que

$$a = s^2 + t^2 + 2u^2 + 2v^2,$$

et

$$b = s + t + 2u + 2v,$$

On a alors :

$$
\begin{aligned}
N &= \frac{m}{2}(a-b)+b, \\
&= \frac{m}{2}\left(s^2+t^2+2u^2+2v^2-s-t-2u-2v\right)+s+t+2u+2v, \\
&= \frac{m}{2}\left(s^2-s\right)+s+\frac{m}{2}\left(t^2-t\right)+t+m\left(u^2-u\right)+2u \\
&\quad +m\left(v^2-v\right)+2v, \\
&= \frac{ms^2-(m-2)s}{2}+\frac{mt^2-(m-2)t}{2}+2\left(\frac{mu^2-(m-2)u}{2}\right) \\
&+4\left(\frac{mv^2-(m-2)v}{2}\right), \\
&= p_{m+2}(s)+p_{m+2}(t)+2p_{m+2}(u)+2p_{m+2}(v).
\end{aligned}
$$

ii) On pose $m=2l$, avec $l \in \mathbb{Z}^+$ est impair.

Soit φ fonction indicatrice d'Euler

l sufit de preuve que pour tout nombres entiers positives

$$
(l-1)^2\frac{4^{k\varphi(l)}-1}{l} \quad (k=1,2,...),
$$

ne pent être écrit comme

$$
P_{m+2}(w)+P_{m+2}(x)+2P_{m+2}(y)+2P_{m+2}(z),
$$

avec w, x, y et $z \in \mathbb{N}$

Soit $n \in \mathbb{Z}^+$, tels que $\varphi(l) \mid n$, supposons qu'il existe w, x, y et $z \in \mathbb{N}$ tels que:

$$
(l-1)^2\,\frac{4^n-1}{l} = P_{m+2}(w)+P_{m+2}(x)+2P_{m+2}(y)+2P_{m+2}(z),
$$

$$
= \frac{2l}{2}\left(w^2+x^2+2y^2+2z^2-w-x-2y-2z\right)+w+x+2y+2z,
$$

alors on a

$$
\begin{aligned}
4^{n+1}(l-1)^2 &= (2lw-(l-1))^2+(2lx-(l-1))^2 \\
&+(2ly-(l-1))^2+(2lz-(l-1))^2, \\
&= (2lw-(l-1))^2+(2lx-(l-1))^2 \\
&+(2l(y+z)-(l-1)^2+2l(y-z))^2,
\end{aligned}
$$

et par conséquence

$$
4^n(l-1)^2 = (lw-\frac{l-1}{2})^2+(lx-\frac{l-1}{2})^2+(l(y+z-1))^2+(l(y-z))^2,
$$

comme

$$4 \mid (l-1)^2$$

on a

$$r_4(4^n(l-1)^2) = r_4\left((l-1)^2\right).$$

D'aprés le lemme (5) il existe $w_0, x_0, y_0, z_0 \in \mathbb{Z}$ tels que

$$w_0^2 + x_0^2 + y_0^2 + z_0^2 = (l-1)^2,$$

alors

$$\begin{aligned} 4^n(l-1)^2 &= 4^n\left(w_0^2 + x_0^2 + y_0^2 + z_0^2\right), \\ &= (2^n w_0)^2 + (2^n x_0)^2 + (2^n y_0)^2 + (2^n z_0)^2 \end{aligned}$$

donc

$$\begin{aligned} lw - \frac{l-1}{2} &= 2^n w_0, \\ lx - \frac{l-1}{2} &= 2^n x_0, \\ l\,(y+z-1)+1 &= 2^n y_0, \\ l\,(y-z) &= 2^n z_0. \end{aligned}$$

D'aprés le théorème 1 d'Euler on a

$$2^{\varphi(l)} = 2^n \equiv 1 (\operatorname{mod} l),$$

donc

$$\begin{aligned} w_0 &\equiv \frac{1-l}{2} \,(\operatorname{mod} l), \\ x_0 &\equiv \frac{1-l}{2} \,(\operatorname{mod} l), \\ y_0 &\equiv 1 \,(\operatorname{mod} l), \\ z_0 &\equiv 0 \,(\operatorname{mod} l). \end{aligned}$$

On a

$$l = \frac{m}{2} \geq 2$$

et par conséquence $w_0, x_0 \neq 0$, alors

$$y_0^2 + z_0^2 \leq (l-1)^2 - 2,$$

donc

$$y_0 \equiv 1(\bmod l) \quad et \quad z_0 \equiv 0 \,(\bmod l)\,,$$

on nécessite trouve $y_0 = 1$ et $z_0 = 0$, comme

$$w_0^2 + x_0^2 + y_0^2 + z_0^2 = (l-1)^2$$

alors

$$w_0^2 + x_0^2 = (l-1)^2 - 1 = l^2 - 2l,$$

comme

$$w_0 \equiv x_0 \equiv \frac{1-l}{2} \,(\bmod l)\,,$$

on nécessité trouve

$$\{w_0, x_0\} \subseteq \{(1-l)/2,\ (1+l)/2\}$$

donc

$$(l-1)^2 = l^2 - 2l,$$

ce contradiction

donc il existe une infinité des nombres entiers ne peut pas ecrit sous la forme

$$P_{m+2}\,(w) + P_{m+2}\,(x) + 2P_{m+2}\,(y) + 2P_{m+2}\,(z)\,.$$

2.2.5 Corollaire 2

On a

$$\{P_5\,(x_1) + P_5\,(x_2) + 2P_5\,(x_3) + 2P_5\,(x_4)\,,\quad x_1, x_2, x_3, x_4 \in \mathbb{N}\} = \mathbb{N} \tag{2.5}$$

$$\{P_6\,(x_1) + P_6\,(x_2) + 2P_6\,(x_3) + 2P_6\,(x_4)\,,\quad x_1, x_2, x_3, x_4 \in \mathbb{N}\} \tag{2.6}$$
$$= \mathbb{N}\backslash \{22, 82, 100\}\,, \tag{2.7}$$

et

$$P_7\,(x_1) + P_7\,(x_2) + 2P_7\,(x_3) + 2P_7\,(x_4)\,,\quad x_1, x_2, x_3, x_4 \in \mathbb{N} \tag{2.8}$$
$$= \mathbb{N}\backslash \{13, 26, 31, 65, 67, 173, 175, 215, 247\}\,,$$

donc

$$\{P_3\,(w) + P_6\,(x) + 2P_6\,(y) + 2P_6\,(z)\,,\ w, x, y, z \in \mathbb{N}\} = \mathbb{N},$$
$$\{2P_3\,(w) + P_6\,(x) + P_6\,(y) + 2P_6\,(z)\,,\ w, x, y, z \in \mathbb{N}\} = \mathbb{N},$$

et

$$\{P_7(w) + P_7(x) + 2P_7(y) + 2P_7(z),\ w \in \mathbb{Z}, x, y, z \in \mathbb{N}\} = \mathbb{N}.$$

Preuve. On applique le théorème (2), pour $m \in \{3, 4, 5, 7, 8, 9\}$ tels que

$$m \nmid 2 \text{ ou } m \mid 4, \text{et } n > 1628m^3$$

alors on peut écrire n comme

$$P_5(n_1) + P_5(n_2) + 2P_5(n_3) + 2P_5(n_4)$$

$$P_6(n_1) + P_6(n_2) + 2P_6(n_3) + 2P_6(n_4)$$

$$P_7(n_1) + P_7(n_2) + 2P_7(n_3) + 2P_7(n_4).$$

On utilisé l'algoritheme $[A]$ pour vérifier (2.5),(2.6)et(2.8) avec

$$n < 1628m^3,$$

et comme peut être ecrit les nombres $\{22, 82, 100\}$ comme

$$\{P_3(n_1) + P_6(y) + 2P_6(z) = x, y, z, w \in \mathbb{N}\}$$

et comme

$$\{2P_3(w) + P_6(x) + P_6(y) + 2P_6(z) = x, y, z, w \in \mathbb{N}\}$$

donc

$$\{P_3(n_1) + P_6(y) + 2P_6(z) + 2P_6(w) = \mathbb{N}\}$$

et

$$\{2p_3(w) + p_6(x) + 2p_6(y) + 2p_6(z) = \mathbb{N}\}$$

et on peut écrit les nombres

$$\{13, 26, 31, 65, 67, 173, 175, 215, 247\}$$

comme

$$p_7(w) + p_7(x) + 2p_7(y) + 2p_7(z), w, t, z, x, y, z \in \mathbb{N},$$

d'ou

$$P_7(w) + P_7(x) + 2P_7(y) + 2P_7(z) = \mathbb{N} \text{ avec } w \in \mathbb{Z} \text{ et } x, y, z \in \mathbb{N}.$$

■

2.3 Troisième formule

Théorème 7 *Soit $m \geq 3$ un nombre entier, pour tout $N \geq 924m^2$, on peut l'écrire sous la forme*

$$P_{m+2}(x_1) + P_{m+2}(x_2) + P_{m+3}(x_3) + 3P_{m+2}(x_4),$$

avec x_1, x_2, x_3 et $x_4 \in \mathbb{N}$.

Pour démontrer ce théorème on a besoin du lemme suivant

2.3.1 Lemme 9

Soit a et b deux nombers entiers vérifient 2.2 et 2.3 pour

$$a \equiv b (\operatorname{mod} 2) \text{ et } a \equiv 3 (\operatorname{mod} 9) \text{ ou } 3 \nmid b,$$

alors il existe $s, t, u, v \in \mathbb{N}$ tels que

$$a = s^2 + t^2 + u^2 + 3v^2,$$
$$b = s + t + u + 3v.$$

Preuve. d'après [3] (pages $112 - 113$)

$$\left\{x^2 + y^2 + 3z^2 : x, y, z \in \mathbb{Z}\right\} = \mathbb{N} \backslash \left\{9^k (9l + 6) : k, l \in \mathbb{N}\right\}, \tag{2.9}$$

si $3 \nmid b$ alors

$$6a - b^2 \equiv 2 (\operatorname{mod} 3),$$

si $a \equiv 3 (\operatorname{mod} 9)$ et $3 \mid b$, alors

$$6a - b^2 \equiv \pm 9 (\operatorname{mod} 27).$$

D'aprés (2.9), on a

$$6a - b^2 = x^2 + y^2 + 3z^2,$$

avec $x, y, z \in \mathbb{Z}$, donc

$$x^2 + y^2 \equiv 2b^2 (\operatorname{mod} 3),$$

alors

$$x \equiv y \equiv b (\operatorname{mod} 3),$$

(si $x \equiv b (\operatorname{mod} 3)$ alors $-x \equiv b (\operatorname{mod} 3)$).
Si a et b sont impairs alors

$$x^2 + y^2 + 3z^2 = 6a - b^2 \equiv 1 (\operatorname{mod} 4),$$

et par conséquent un de x et y est impair.

Si a et b sont pairs alors

$$x^2 + y^2 + 3z^2 = 6a - b^2 \equiv 0 \pmod 4,$$

et par conséquent un de x et y est pair.

On peut suppose que

$$x \equiv a \equiv b \pmod 2,$$

et

$$y \equiv z \pmod 2,$$

alors tout les nombres

$$\begin{aligned} s &= \frac{b+x+y+3z}{6}, \\ t &= \frac{b+x+y-z}{6}, \\ u &= \frac{b+x-2y}{6}, \\ v &= \frac{b-x}{6}, \end{aligned}$$

sont des nombres entiers.

On va montrer que $s, t, u, v \in \mathbb{N}$,

on remarque que

$$s + t + u + 3v = \frac{b+v}{2} + 3\frac{b-x}{6} = b,$$

et

$$\begin{aligned} s^2 + t^2 + u^2 + 3v^2 &= 2\left(\frac{s+t}{2}\right)^2 + 2\left(\frac{s-t}{2}\right)^2 + u^2 + 3v^2 \\ &= 2\left(\frac{b+x+y}{6}\right)^2 + 2\left(\frac{z}{2}\right)^2 + \left(\frac{b+x-2y}{6}\right)^2 + 3\left(\frac{b-v}{6}\right)^2 \\ &= \frac{b^2+x^2+y^2+3z^2}{6} = a. \end{aligned}$$

D'aprés le lemme (3)

$$(|x| + |y| + 3|z|)^2 \leq 5\left(x^2 + y^2 + 3z^2\right) = 5(6a - b^2) < (b+6)^2.$$

par conséquent

$$b - |x| - |y| - 3|z| > -6,$$

donc

$$s, t, u, v \geq \frac{b - |x| - |y| - 3|z|}{6} > 1,$$

d'où $s, t, u, v \in \mathbb{N}$. ■

2.3.2 Démonstration du théorème (3)

On a

$$\begin{aligned} N \geq 924m^2 &= 99m^3(9+\frac{1}{3}) \geq 99m^3(9+\frac{1}{m}) \\ &= 99m^2(9m+1), \end{aligned}$$

la longueur de l'intervalle $I_2 = [\alpha, B]$, définit sur le lemme (6) est superieur à $9m$,

soit

$$b_0 \in \{[\alpha] + r : r = 0, 1, ..., m-1\},$$

tels que

$$b_0 \equiv N (\operatorname{mod} m).$$

Si $3 \nmid m$ ou $3 \nmid N$, alors on peut choisit

$$b_0 \in \{b_0, b_0 + m\}$$

tels que

$$b \not\equiv 0 (\operatorname{mod} 3).$$

Pour $3 \mid m$ et $3 \mid N$, soit

$$c_0 \in \{[\alpha] + r : r = 0, 1, ..., 3m-1\},$$

tels que

$$b_0 \equiv N (\operatorname{mod} 3m),$$

et soit

$$b = c_0 + j3m,$$

tels que $j = \{1.2.3\}$,

on a

$$\frac{2}{m}(N - c_0) + c_0 - bj \equiv 3 (\operatorname{mod} 9),$$

notons que $b \in I_2$ puis que

$$a \leq b \leq [\alpha] + 3m - 1 + 6m < \alpha + 9m < \beta.$$

Soit

$$a = \frac{2}{m}(N - b) + b,$$

c.à.d

$$N = \frac{m}{2}(a+b) + b,$$

alors

$$a = \frac{2N}{m} + \left(1 - \frac{2}{m}\right) b > 0,$$

et

$$a \equiv b (\operatorname{mod} 2).$$

Si $3 \mid b$ alors $3 \mid m$, et

$$\begin{aligned} a &= \frac{2}{m}(N-b) + b \\ &= \frac{2}{m}(N - c_0 - 3jm) + c_0 + 3jm \\ &\equiv \frac{2}{m}(N - c_0) + -6j \\ &\equiv 3 (\operatorname{mod} 9). \end{aligned}$$

D'aprés le lemme (7) et le lemme (9), il existe s, t, u et $v \in \mathbb{N}$ tels que

$$\begin{cases} a = s^2 + t^2 + u^2 + 3v^2 \\ b = s + t + u + 3v, \end{cases}$$

donc

$$\begin{aligned} & N = \frac{m}{2}(a-b) + b \\ & = \frac{m}{2}\left(s^2 + t^2 + u^2 + 3v^2 - s - t - u - 3v\right) + s + t + u + 3v \\ & = \frac{m}{2}\left(s^2 - s\right) + s + \tfrac{m}{2}\left(t^2 - t\right) + t + \tfrac{m}{2}\left(u^2 - u\right) + u \\ & +3\tfrac{m}{2}\left(v^2 - v\right) + 3v \end{aligned}$$

$$\begin{aligned} N = & \frac{ms^2 - (m-2)s}{2} + \frac{mt^2 - (m-2)t}{2} + \frac{mu^2 - (m-2)u}{2} \\ & + 3\left(\frac{mv^2 - (m-2)v}{2}\right), \\ & = P_{m+2}(s) + P_{m+2}(t) + P_{m+2}(u) + 3P_{m+2}(v). \end{aligned}$$

2.3.3 Corollaire 3

On a

$$\{P_5(x_1) + P_5(x_2) + P_5(x_3) + 3P_5(x_4), \quad x_1, x_2, x_3, x_4 \in \mathbb{N}\} = \mathbb{N} \backslash \{19\} \tag{2.10}$$

$$\{P_6(x_1) + P_6(x_2) + P_6(x_3) + 3P_6(x_4), \quad x_1, x_2, x_3, x_4 \in \mathbb{N}\} \tag{2.11}$$

$$= \mathbb{N} \backslash \{14, 23, 41, 42, 83\} \tag{2.12}$$

et

$$P_7(x_1)+P_7(x_2)+P_7(x_3)+3P_7(x_4), \quad x_1,x_2,x_3,x_4\in\mathbb{N} \tag{2.13}$$
$$=\mathbb{N}\backslash\{13,16,27,31,33,49,50,67,87,178,181,259\},$$

On a

$$\begin{aligned}&P_9(x_1)+P_9(x_2)+P_9(x_3)+3P_9(x_4), \quad x_1,x_2,x_3,x_4\in\mathbb{N}\\&=\mathbb{N}\backslash\{17,21,34,41,67,89,104,119,170,237,245,290\},\end{aligned} \tag{2.14}$$

et on a pour $k=8,9,10$ et pour tout nombre entier $n>N_k$, on peut écrit n comme

$$P_k(x_1)+P_k(x_2)+P_k(x_3)+3P_k(x_4), \quad x_1,x_2,x_3,x_4\in\mathbb{N}, \tag{2.15}$$

tels que $N_8=435$, $N_9=695$ et $N_{12}=916$, alors

$$\{P_7(x_1)+P_7(x_2)+P_7(x_3)+3P_7(x_4), \quad x_1\in\mathbb{Z} \text{ et } x_2,x_3,x_4\in\mathbb{N}\}=\mathbb{N}, \tag{2.16}$$

$$\begin{aligned}&P_9(x_1)+P_9(x_2)+P_9(x_3)+3P_9(x_4), \quad x_1,x_2,x_3,x_4\in\mathbb{N}\\&=\mathbb{N}\backslash\{17\},\end{aligned}$$

$$\begin{aligned}&P_{10}(x_1)+P_{10}(x_2)+P_{10}(x_3)+3P_{10}(x_4), \quad x_1,x_2,x_3,x_4\in\mathbb{N}\\&=\mathbb{N}\backslash\{16,19\},\end{aligned} \tag{2.17}$$

Preuve. On applique le théoreme (3), pour $m\in\{3,4,5,6,7,8\}$ tels que $n>924m^3$, alors n peut être écrit comme

$$P_k(x_1)+P_k(x_2)+2P_k(x_3)+4P_k(x_4), \quad x_1,x_2,x_3,x_4\in\mathbb{N},$$

pour $k\in\{5,6,7,,8,9,10\}$.

Si $n<924m^3$ on utilisé l'algorithme $[A]$ pour vérifier (2.10) et (2.17). ■

2.4 Quatrième formule

Théorème 8 *Soient $m,N\in\mathbb{Z}$ tels que $m\geq 3$, alors $\forall N\geq 1056m^3$, on peut écrire N sous la forme*

$$P_{m+2}(x_1)+P_{m+2}(x_2)+2P_{m+3}(x_3)+4P_{m+2}(x_4),$$

avec $x_1,x_2,x_3,x_4\in\mathbb{N}$.

Pour démontrer ce théorème on a besoin des lemmes suivants

2.4.1 Lemme 10

Soient $l, m, N \in \mathbb{Z}^+$, tels que $lm \geq 20$ et $N \geq 3lm^2(5lm + 12)$, alors

la longueur de l'intervalle

$$I_4 = \left[\frac{5}{2} + \sqrt{\frac{14N}{m} - 1}, \frac{4}{3} + 4\sqrt{\frac{N}{m}}\right],$$

est supérieur à lm.

Preuve. Soit L_4 la longueur de l'intervalle I_4

$$L_4 = 4\sqrt{x} - \sqrt{14x - 1} - \frac{7}{6}, \text{ où } x = \frac{N}{m}.$$

soit $l_0 = lm + \frac{7}{6}$, on a alors

$$\begin{aligned} L_4 > lm \quad &\Longleftrightarrow 4\sqrt{x} > \sqrt{14x - 1} + l_0 \\ &\Longleftrightarrow 2x + 1 - l_0^2 < 2l_0\sqrt{14x - 1} \\ &\Longleftrightarrow 4x(x + 1 - 15l_0^2) + (l_0^2 - 1)^2 + 4l_0^2 > 0, \end{aligned}$$

comme

$$\begin{aligned} x \quad &\geq 15l^2m^2 + 36lm \\ &> 15l^2m^2 + 35lm + \frac{245}{12} - 1 \\ &= 15l_0^2 - 1, \end{aligned}$$

donc

$$L_4 > lm.$$

■

2.4.2 Lemme 11

Soient a, b, m, $N \in \mathbb{Z}$, tels que $m \geq 3$ et

$$b \in I_4 N = \frac{m}{2}(a - b) + b \geq \frac{4}{7}m,$$

Soit I_4 l'intervalle donnée sur lemme (10), alors

$$b^2 < 8a, \tag{2.18}$$

et

$$7a \ < b^2 + 2b + 8, \tag{2.19}$$

Preuve.

Pour démontrer (2.18) il suffit de démontrer que:

$$b^2 - 8a < 0,$$

on a

$$a = (1 - \frac{2}{m})b + \frac{2N}{m}$$

alors

$$b^2 - 8a = b^2 - 8(1 - \frac{2}{m})b - \frac{16N}{m}$$

c'est est une fourmule quadratique:

$$\triangle = 8^2(1 - \frac{2}{m})^2 + \frac{72N}{m} > 0,$$

et les racines sont:

$$b_1 = 4(1 - \frac{2}{m}) + 4\sqrt{(1 - \frac{2}{m})^2 + \frac{N}{m}},$$

$$b_2 = 4(1 - \frac{2}{m}) - 4\sqrt{(1 - \frac{2}{m})^2 + \frac{N}{m}}.$$

Alors

$$b^2 - 6a < 0$$

si

$$0 < b < 4(1 - \frac{2}{m}) + 4\sqrt{(1 - \frac{2}{m})^2 + \frac{N}{m}},$$

et comme $b \in I_2$ alors:

$$\begin{aligned} 0 < b \quad &< \frac{4}{3} + 4\sqrt{\frac{N}{m}} \\ &\leq 4(1 - \frac{2}{m}) + 4\sqrt{(1 - \frac{2}{m})^2 + \frac{N}{m}}. \end{aligned}$$

Donc $I_4 \subset [b_1, b_2]$ alors

$$\forall b \in I \Longrightarrow b^2 - 8a > 0,$$

c'est la preuve de (2.18).Pour montrer (2.19) il suffit de montrer que:

$$b^2 + 2b + 8 - 7a > 0.$$

On étude le signe de la formule quadratique

$$\begin{aligned} &b^2 + 2b + 8 - 7a \\ &= b^2 - (5 - \frac{14}{m})b + (8 - \frac{14N}{m}), \end{aligned}$$

$$\triangle = (5 - \frac{14}{m})^2 - (8 - \frac{14N}{m}) > 0,$$

car

$$(8-\frac{14N}{m})<0$$

$$b_1=(\frac{5}{2}-\frac{7}{m})+\sqrt{(\frac{5}{2}-\frac{7}{m})^2+\frac{14N}{m}-8},$$

$$b_2=(\frac{5}{2}-\frac{7}{m})-\sqrt{(\frac{5}{2}-\frac{7}{m})^2+\frac{14N}{m}-8},$$

alors:

$$b^2+2b+8-7a>0.$$

Si $b\in\mathbb{R}\backslash\{b_1,b_2\}$ comme $b\in I_4$alors:

$$\begin{aligned} b &\geq \frac{5}{2}+\sqrt{\frac{14N}{m}-1} \\ &\geq (\frac{5}{2}-\frac{7}{m})+\sqrt{(\frac{5}{2}-\frac{7}{m})^2+\frac{14N}{m}-8} \\ &= b_1, \end{aligned}$$

donc $b\in I\Longrightarrow b^2+2b+8-7a>0$. C'est la preuve de (2.19.)

■

2.4.3 Lemme 12

Soit $a,b\in\mathbb{Z}^+$ vérifient , (2.18) et (2.19), supposons que

1) $2\nmid ab$,

ii) $2\mid a$ et $2\parallel b$,

iii) $4\mid a$ et $4\parallel b$, ou $a\equiv b+4(\bmod 16)$ et $8\mid b$,

alors il éxiste $s,t,u,v\in\mathbb{N}$ tels que:

$$a=s^2+t^2+2u^2+4v^2 \text{ et } b=s+t+2u+4v.$$

Preuve. d'après [3] (pages $112-113$)

on a

$$\left\{x^2+2y^2+4z^2 : x,y,z\in\mathbb{Z}\right\}=\mathbb{N}\backslash\left\{4^k\left(16l+14\right):k,l\in\mathbb{N}\right\} \tag{2.20}$$

comme $8a-b^2\neq 4^k(16l+14)$, alors il éxiste $x,y,z\in\mathbb{Z}$, tels que

$$8a-b^2=x^2+2y^2+4z^2$$

et

$$a = \frac{x^2 + 2y^2 + 4z^2 + b^2}{8}.$$

Soit les nombres suivantes

$$\begin{aligned} u &= \frac{b + x - 2y}{8} \\ v &= \frac{b - x}{8} \\ s &= u + \frac{b + z}{2} \\ t &= u + \frac{y - z}{2}. \end{aligned} \tag{2.21}$$

nous allons démontrer que u, s, t, u et $v \in \mathbb{N}$. pour les cas: i), ii) et iii).

Cas 1 $2 \nmid ab$

On a a et b sont des impairs, donc

$$b \equiv 1 (\operatorname{mod} 2) \implies -b^2 \equiv -1 (\operatorname{mod} 4) \equiv -1 (\operatorname{mod} 8)$$

donc

$$8a - b^2 \equiv -1 (\operatorname{mod} 8)$$

alors

$$x^2 + 2y^2 + 4z^2 \equiv -1 (\operatorname{mod} 8) \implies x^2 + 2y^2 + 4z^2 + b^2 \equiv 0 (\operatorname{mod} 8),$$

d'ou $a \in \mathbb{Z}$.

On a

$$\begin{cases} x^2 + 2y^2 + 4z^2 \equiv -1 (\operatorname{mod} 8) \equiv -1 (\operatorname{mod} 4), \\ 4z^2 \equiv 0 (\operatorname{mod} 4), \end{cases}$$

donc

$$x^2 + 2y^2 \equiv -1 (\operatorname{mod} 4)$$

alors $2 \nmid xy$ et on a

$$4z^2 \equiv 0 (\operatorname{mod} 4) \equiv -4 (\operatorname{mod} 8),$$

donc

$$z^2 \equiv -1 (\operatorname{mod} 8),$$

alors $2 \nmid z$, et comme $2 \nmid xy$, on déduire que $2 \mid y \pm z$

d'ou $s, t \in \mathbb{Z}$.

D'autre coté on a

$$\begin{aligned} x^2 &= 8a - 2y^2 - 4z^2 = 8 - b^2 - 2 - 4, \\ &= 2 - b^2 \equiv b^2 (\operatorname{mod} 16), \end{aligned} \tag{2.22}$$

alors
$$x \equiv \pm b (\bmod 8),$$
donc
$$b - x \equiv 0 (\bmod 8),$$
d'ou $v \in \mathbb{Z}$, d'après (2.22) on a
$$\begin{cases} x \equiv -b (\bmod 8) \\ y \equiv b (\bmod 4) \end{cases} \Longrightarrow \begin{array}{c} x \equiv -b (\bmod 8) \\ -2y \equiv -2b (\bmod 8) \end{array}$$
$$\Longrightarrow x + b - 2y \equiv 0 (\bmod 8),$$

donc $u \in \mathbb{Z}$

Cas 2 $2 \mid a$ et $2 \parallel b$

On pose $a = 2a_0$ et $b = 2b_0$ tels que $a_0, b_0 \in \mathbb{Z}$ et $2 \nmid b_0$

on a
$$4a_0 - b_0^2 \equiv 3 (\bmod 4),$$
car
$$4a_0 \equiv 0 (\bmod 4) \text{ et } - b_0^2 \equiv 3 (\bmod 4),$$
d'après(2.20)on a
$$4a_0 - b_0^2 = x_0^2 + 2y_0^2 + 4z_0^2,$$
pour tous $x_0, y_0, z_0 \in \mathbb{Z}$

alors
$$x_0^2 + 2y_0^2 + 4z_0^2 \equiv 3 (\bmod 4) \Longrightarrow x_0^2 + 2y_0^2 \equiv 3 (\bmod 4),$$
si et seulement si x_0 et y_0 sont des impairs, alors les deux x et y sont des pairs

et on a
$$4z_0^2 \equiv 0 (\bmod 4) \equiv -4 (\bmod 8),$$
donc
$$z_0^2 \equiv -1 (\bmod 8),$$
alors $2 \nmid z_0 \Longrightarrow 2 \mid z$ pour $z = 2z_0$, et comme $y \mid 2$, on déduire que $2 \mid y \pm z$, donc $s, t \in \mathbb{Z}$.

Ensuite
$$\begin{cases} x_0^2 + 2y_0^2 \equiv 3 (\bmod 4) \\ -2y_0^2 \equiv -2 (\bmod 4) \end{cases} \Longrightarrow x_0^2 \equiv 1 (\bmod 4),$$

et

$$b \equiv 2 (\bmod 4) \Longrightarrow b_0^2 \equiv 1 (\bmod 4),$$

$$\begin{aligned} y_0 \equiv 1 (\bmod 2) &\Longrightarrow 2y_0^2 \equiv 2 (\bmod 4) \\ &\Longrightarrow y_0^2 \equiv 1 (\bmod 4), \end{aligned}$$

alors

$$x_0^2 \equiv y_0^2 \equiv b_0^2 (\bmod 4),$$

donc

$$x_0 \equiv y_0 \equiv b_0 (\bmod 4),$$

alors

$$x \equiv y \equiv b (\bmod 8),$$

pour $y = 2y_0$et $z = 2x_0$, d'ou $u, v \in \mathbb{N}$

Cas 3 $4 \mid a$ et $4 \parallel b$,ou $a \equiv b + 4 (\bmod 16)$ et $8 \mid b$

On pose $a = 4a_0$ et $b = 4b_0$ pour $a_0, b_0 \in \mathbb{Z}$

$$2a_0 - b_0^2 \equiv \begin{cases} 1 (\bmod 2) & \text{si} 4 \parallel b \ \ (2 \nmid b_0) \\ 2 (b_0 + 1) - b_0^2 \equiv 2 (\bmod 8) \equiv 0 (\bmod 2) & \text{si } a \equiv b + 4 (\bmod 16) \text{ et } 8 \mid b \end{cases}$$

d'après (2.20)

$$2a_0 - b_0^2 = x_0^2 + 2y_0^2 + 4z_0^2,$$

pour $x_0, y_0, z_0 \in \mathbb{Z}$

On remarque que

$$x_0^2 \equiv \begin{cases} 1 (\bmod 2) & \text{si} 4 \parallel b \ \ (2 \nmid b_0) \\ 0 (\bmod 2) & \text{si } a \equiv b + 4 (\bmod 16) \text{ et } 8 \mid b \end{cases},$$

et

$$b_0^2 \equiv \begin{cases} 1 (\bmod 2) & \text{si} 4 \parallel b \ \ (2 \nmid b_0) \\ 0 (\bmod 2) & \text{si } a \equiv b + 4 (\bmod 16) \text{ et } 8 \mid b \end{cases},$$

donc

$$\begin{aligned} x_0 \equiv b_0 (\bmod 2) &\Longrightarrow x \equiv b (\bmod 8) \\ &\Longrightarrow b \pm x \equiv 0 (\bmod 8), \end{aligned}$$

d'ou $v \in \mathbb{Z}$

et comme $2y_0 \equiv 0 (\mod 2)$

alors

$$b_0 + x_0 - 2y_0 \equiv 0(\mod 2) \Longrightarrow b + x - 2y \equiv 0(\mod 8),$$

donc $u \in \mathbb{Z}$

on a

$$4y_0 \pm 4z_0 \equiv 0(\mod 2) \Longrightarrow y \pm z0(\mod 2),$$

donc $s, t \in \mathbb{Z}$

d'ou $s, t, u, v \in \mathbb{Z}$ pour tous les cas $i), ii)$ et $iii)$.

Il reste de démonrer que $s, t, u, v \in \mathbb{N}$

On a

$$\begin{aligned} s + t + 2u + 4v &= y + 2u + 2u + 4v, \\ &= \frac{b+x}{2} + \frac{b-x}{2} = b, \end{aligned}$$

et

$$\begin{aligned} & s^2 + t^2 + 2u^2 + 4v^2 \\ & = 2\left(u + \frac{y}{2}\right)^2 + 2\left(\frac{z}{2}\right)^2 + 2\left(\frac{b+x-2y}{8}\right)^2 + 4\left(\frac{b-x}{8}\right)^2, \\ & = 2\left(\frac{b+x+2y}{8}\right)^2 + 2\left(\frac{b+x-2y}{8}\right)^2 + \frac{z^2}{2} + \left(\frac{b-x}{4}\right)^2, \\ & = \left(\frac{b+x}{4}\right)^2 + \left(\frac{y}{2}\right)^2 + \frac{z^2}{2} + \left(\frac{b-x}{4}\right)^2, \\ & \frac{x^2 + 2y^2 + 4z^2 + b^2}{8} = a. \end{aligned}$$

D'après les lemmes (3) et (11) on a

$$\begin{aligned} (|x| + 2|y| + 4|z|)^2 &\leq 7\left(x^2 + 2y^2 + 4z^2\right) \\ &= 7\left(8a - b^2\right) < (b+8)^2, \end{aligned}$$

alors

$$b - |x| - 2|y| - 4|z| > -8,$$

alors

$$u, v, s, t \geq \frac{b - |x| - 2|y| - 4|z|}{8} > -1 \geq 0,$$

alors s, t, u et $v \in \mathbb{N}$.

■

2.4.4 Démonstration du théorème (4)

On a

$$\begin{aligned} N &\geq 96m^2 \times 11m \geq 96m^2 (10m+3) \\ &= 24m^2 (40m+12), \end{aligned}$$

on applique le lemme (10) pour $l = 8$

alors la longueur de l'intervalle donnée sur le lemme (10)

$$I_4 = [\alpha, \beta],$$

est supérieur à 8 m.

1. $4 \nmid m$ ou $8 \nmid N$

   On pose

   $$b_0 \in \{[\alpha] + r : r = 0, 1, ..., m-1\}$$

   tels que

   $$N \equiv b_0 (\operatorname{mod} m)$$

   soit $b_1 = b_0 + m$alors

   $$\alpha \leq b_0 < b_1 \leq [\alpha] + 2m - 1 < \alpha + 8m < \beta$$

   alors $b_j \in I_4$ pour $j = 0, 1$. On note

   $$a_j = \frac{2}{m}(N - b_j) + b_j = \frac{2}{m}(N - b_0) + b_0 + (m-2)j.$$

   Si $2 \nmid m$ alors

   $$a_j \equiv b_j \equiv 1 (\operatorname{mod} 2).$$

   Si $2 \mid m$ et $2 \nmid N$

   alors

   $$a_0 \equiv b_0 \equiv 1 (\operatorname{mod} 2).$$

   Si $2 \parallel m$ et $2 \mid N$

   alors

   $$b_j \equiv 2 (\operatorname{mod} 4) \text{ et } 2 \mid a_j$$

   donc

   $$4 \mid m \text{ et } 2 \parallel N$$

d'ou

$$a_0 \equiv b_0 \equiv 0 (\mathrm{mod}\, 2) \text{ et } b_0 \equiv 2 (\mathrm{mod}\, 4).$$

Si $4 \parallel m$ et $4 \parallel N$

alors $4 \mid b_0$

et pour $j \in \{0, 1\}$, on a

$$b_j \equiv 4 (\mathrm{mod}\, 8) \text{ et } a_j \equiv b_j \equiv 0 (\mathrm{mod}\, 4).$$

alors $8 \mid m$ et $4 \parallel N$

on a alors

$$b_0 \equiv 4 (\mathrm{mod}\, 8) \text{ et } a_0 \equiv b_0 (\mathrm{mod}\, 2)$$

d'ou

$$a_j \equiv 0 (\mathrm{mod}\, 4) \text{ et } b_j \equiv 4 (\mathrm{mod}\, 8)$$

2. $4 \mid m$ et $8 \mid N$

   on pose

$$b \in \{[\alpha] + r : r = 0, 1, ..., 8m - 1\}$$

   tels que

$$b \equiv N - 2m (\mathrm{mod}\, 8m)$$

   alors

$$\alpha \leq b \leq [\alpha] + 8m - 1 < \alpha + 8m < \beta$$

   donc $b \in I_4$

   on a

$$8 \mid b \Longrightarrow 8 \mid N \text{ et } 4 \mid m.$$

   donc

$$\frac{2}{m} (N - b) + b \equiv 4 + b (\mathrm{mod}\, 8).$$

alors pour tous les cas nous pouvons toujours trouver $b \in I_4$ et $a \in \mathbb{Z}$

pour quel un de (i)-(ii) dans le lemme (12)

et on a

$$a = \frac{2}{m} (N - b) + b \text{ i.e, } N = \frac{m}{2} (a - b) + b.$$

D'après les lemmes (11) et (12), il existe s, t, u et $v \in \mathbb{N}$ tels que

$$\begin{cases} a = s^2 + t^2 + 2u^2 + 4v^2 \\ b = s + t + 2u + 4v, \end{cases}$$

donc

$$\begin{aligned}
N &= \tfrac{m}{2}(a-b)+b, \\
&= \frac{m}{2}\left(s^2+t^2+2u^2+4v^2-s-t-2u-4v\right)+s+t+2u+4v, \\
&= \frac{m}{2}\left(s^2-s\right)+s+\frac{m}{2}\left(t^2-t\right)+t+m\left(u^2-u\right)+2u \\
&+2m\left(v^2-v\right)+4v,
\end{aligned}$$

$$\begin{aligned}
N = {} & \frac{ms^2-(m-2)s}{2}+\frac{mt^2-(m-2)t}{2}+2\left(\frac{mu^2-(m-2)u}{2}\right) \\
& +4\left(\frac{mv^2-(m-2)v}{2}\right) \\
& = p_{m+2}(s)+p_{m+2}(t)+2p_{m+2}(u)+4p_{m+2}(v).
\end{aligned}$$

2.4.5 Corollaire 4

On a

$$\{P_5(x_1)+P_5(x_2)+2P_5(x_3)+4P_5(x_4),\quad x_1,x_2,x_3,x_4\in\mathbb{N}\}=\mathbb{N}, \tag{2.23}$$

$$\{P_6(x_1)+P_6(x_2)+2P_6(x_3)+4P_6(x_4),\quad x_1,x_2,x_3,x_4\in\mathbb{N}\}=\mathbb{N},$$

et

$$\begin{aligned}
& P_7(x_1)+P_7(x_2)+2P_7(x_3)+4P_7(x_4),\quad x_1,x_2,x_3,x_4\in\mathbb{N} \\
& =\mathbb{N}\backslash\{17,51\},
\end{aligned} \tag{2.24}$$

$$\begin{aligned}
& P_8(x_1)+P_8(x_2)+2P_8(x_3)+4P_8(x_4),\quad x_1,x_2,x_3,x_4\in\mathbb{N} \\
& =\mathbb{N}\backslash\{19,30,39,59,78,91\},
\end{aligned} \tag{2.25}$$

$$\begin{aligned}
& P_9(x_1)+P_9(x_2)+2P_9(x_3)+4P_9(x_4),\quad x_1,x_2,x_3,x_4\in\mathbb{N} \\
& =\mathbb{N}\backslash\{17,21,34,41,67,89,104,119,170,237,245,290\},
\end{aligned} \tag{2.26}$$

et on a pour $k=10,11,12$,et pour tout nombre entier $n>N_k$, on peut écrire n comme

$$P_k(x_1)+P_k(x_2)+2P_k(x_3)+4P_k(x_4),\quad x_1,x_2,x_3,x_4\in\mathbb{N} \tag{2.27}$$

où $N_{10}=333$, $N_{11}=734$ et $N_{12}=1334$, alors

$$\{P_k(x_1)+P_k(x_2)+2P_k(x_3)+4P_k(x_4),\quad x_1\in\mathbb{Z}\text{ et }x_2,x_3,x_4\in\mathbb{N}\}=\mathbb{N} \tag{2.28}$$

pour $k=7,9$

$$\{P_k(x_1)+P_k(x_2)+2P_k(x_3)+4P_k(x_4),\quad x_1,x_2,x_3,x_4\in\mathbb{N}\}=\mathbb{N}, \tag{2.29}$$

pour $k = 8, 10, 11.12$.

Preuve. On applique le théoreme (4),pour $m \in \{3,4,5,6,7,8,9,10\}$ et $n > 1056m^3$, alors n peut être écrit comme :

$$P_k(x_1) + P_k(x_2) + 2P_k(x_3) + 4P_k(x_4), \quad x_1, x_2, x_3, x_4 \in \mathbb{N},$$

pour $k \in \{5, 6, 7, , 8, 9, 10, 11, 12\}$,

Si $n < 1056m^3$,on utilise l'algorithme $[A]$. ■

2.5 L'algorithme $[A]$.

```
Debut
     variable    n,i,j,k,l entier
     lire n ;
     lire P1 ;
     lire P2 ;
     lire P3 ;
     lire P4 ;
     pour   i=1 à n
         faire
              pour j=1 à n
                  faire
                   pour k=1 à n
                       faire
                              pour l=1 à n
                                  faire
                                   a  := P1(l)
                                   b  := P2(l)
                                   c  := P3(l)
                                   d  := P4(l)
                                   A= a + b + c + d
                                   Si    A < >   Trunc  (A)
                                  Alors          écrire  (A)
                         fin
                      fin
                   fin
                fin
  fin
```

Bibliographie

[1] **B.C.Berndt**,Number theory in the Spirit of Ramanujan, amer. Math.Soc, Providence,RI.,2006.

[2] **L.E.Dickson,**Quaternary quadratic forms representing all integers, amer. J. Math. 49 (1927),

[3] **L.E.Dickson,**Modern Elementary theory of Nuumbers,Université de Chicago,chicago,1993

[4] **F. Ge and Z.-W. Sun.**, On some universal sums of generalized polygonals, Colloq. Math. 145 (2016), 149–155.

[5] **R. K. Guy** , Every number is expressible as the sum of how many polygonal numbers? Amer. Math. mensuel 101 (1994), 169–172.

[6] **D. KrachunG**, On sums of triangular numbers, preprint, arXiv:1602.01133, 2016.

[7] **C. J. Moreno and S**. S. Wagstaff, Sums of Squares of Integers, Chapman , FL, 2006.

[8] **M. B. Nathanson** , A short proof of Cauchy's polygonal number theorem, Proc. Amer. Math. Soc. 99 (1987), 22–24.

[9] **M. B. Nathanson**, Additive Number Theory: The Classical Bases, Grad. Textes dans Math., vol. 164, Springer, New York, 1996.

[10] **S. Ramanujan**, On the expression of a number in the form $ax^2 + by^2 + cz^2 + dw^2$,

[11] **Z.-W. Sun**, On universal sums of polygonal numbers, Sci. Chine Math. 58 (2015), 1367–1396.

[12] **Z.-W. Sun.**, A result similar to Lagrange's theorem, J. Number Théorie de nombre 162 (2016), 190–211.

[13] **Bulletin AMQ**, Vol. XLVI, n^{0}3, octobre 2006 **.**