Nombre entier somme de deux carrés. Combien de façons ?

Tout nombre entier positif n se décompose en produit de nombres premiers de façon unique. Cela peut s'écrire :

$n = 2^a \prod p^{b_i} \prod p'^{c_j}$ où p et p' sont des nombres premiers impairs, avec $p = 1$ [4] et $p' = 3$ [4] (ce qui signifie que $p = 4k + 1$ et $p' = 4k' + 3$). On distingue ici deux types de nombres premiers impairs.

Notre objectif est d'écrire n comme somme de deux carrés de nombres entiers, soit $n = x^2 + y^2$, et de connaître le nombre R de couples (x, y) possibles pour n donné. Autrement dit, R est le nombre de façons de représenter n comme somme de deux carrés. On appellera aussi R' le nombre de cas au signe et à l'ordre près pour x et y, ce qui signifie que l'on peut prendre $x \geq y \geq 0$. Par exemple :

pour $n = 3$, $R = 0$.
pour $n = 5$, $5 = (\pm 2)^2 + (\pm 1)^2$ ou $(\pm 1)^2 + (\pm 2)^2$, soit $R = 8$ et $R' = 1$.
pour $n = 25 = 5^2$, $25 = (\pm 5)^2 + 0^2$ ou $(\pm 4)^2 + (\pm 3)^2$ à l'ordre près, soit $R = 12$ et $R' = 2$.
pour $n = 50 = 2 \times 5^2$, $50 = (\pm 5)^2 + (\pm 5)^2$ ou $(\pm 7)^2 + (\pm 1)^2$ à l'ordre près, soit $R = 12$ et $R' = 2$.

On constate que $R' = R / 8$ si et seulement si on n'a pas $x = y$ ou $y = 0$. Lorsque $x = y$ ou $y = 0$, seuls 4 cas dans R donnent un cas pour R'. Notamment, si n est un carré de la forme p^b avec b pair[1], on a $R' = (R + 4)/8$. Et de même si $n = x^2 + x^2$.

On dispose alors de la propriété suivante[2] :

> Si tous les exposants c_i (des nombres premiers p') sont pairs, alors $R = 4 \prod (b_i + 1)$ où les b_i sont les exposants des nombres premiers p.

On vérifie qu'avec $p' = 4k + 3$, soit $p' = 3$ [4], $p'^c = 1$ [4] si c est pair, et $p'^c = 3$ [4] si c est impair.
On vérifie aussi que si $p = 1$ [4], $p^b = 1$ [4]. Il découle alors de la propriété précédente que

* si n est un nombre impair tel que $n = 3$ [4], n contient des p' à une puissance impaire, et $R = 0$.
* si n est un nombre impair tel que $n = 1$ [4], n contient des p' tous à une puissance paire, et $R = 4 \prod (b_i + 1)$.
* si n est pair avec $n = 2^a n'$ ($a > 0$) et $n' = 3$ [4], $R = 0$.
* si n est pair avec $n = 2^a n'$ ($a > 0$) et $n' = 1$[4], $R = 4 \prod (b_i + 1)$.

En particulier, si n est un nombre premier impair de la forme $4k + 3$, $R = 0$, et s'il est de la forme $4k + 1$, $R = 8$ et $R' = 1$.

Les nombres p de la forme $4k + 1$ sont les seuls à pouvoir rendre $R > 0$. Les premiers de ces nombres sont 5, 13, 17, 29, 37, 41, 53, 57, etc.

Dans certains cas, on dispose de la propriété supplémentaire :

---

[1] Par exemple pour $15625 = 5^6$, on trouve $R = 28$ et $R' = 4$, avec les solutions (125, 0), (120,35), (117,44), (100, 75). Par contre si l'on a p^b avec b impair, on trouve que R est divisible par 8 avec $R' = R/8$. Par exemple pour $3125 = 5^5$, on trouve $R = 24$ et $R' = 3$, avec les solutions (55, 10), (50 , 25), (41,30).

[2] Voir par exemple le classique de Niven, Zuckerman, Montgomery, *An introduction to the theory of numbers*,

Si a (exposant de 2) vaut 0 ou 1, le nombre r de représentations de n comme somme de deux carrés (x , y) où x est premier avec y, est égal à 2^{t+2} où t est le nombre des nombres premiers p de la forme $4k + 1$ présents dans la décompossition de n. En appelant r' le nombre de représentations au signe et à l'ordre près (soit $x > y > 0$), on a toujours $r' = r/8$.

Par exemple, pour $n = 50 = 2 \times 5^2$, $r = 2^3 = 8$, soit $(\pm 7)^2 + (\pm 1)^2$ à l'ordre près comme on l'a vu précédemment, ou encore $r' = 1$, avec $50 = 7^2 + 1^2$.

Exercice 1 : *Parmi tous les nombres n inférieurs à 1000, quelle est la plus grande valeur de R (ou R') ainsi que celle de r.Et parmi tous les nombres n inférieurs à 2000 ?*

En prenant un seul nombre premier p, ici une puissance de 5 maximale, soit $5^4 < 1000$ et 2000, on trouve $R = 20$ et $R' = 8$. En effet $625 = 5^4 = 25^2 + 0^2$ ou $24^2 + 7^2$ ou $20^2 + 15^2$. On a aussi $r = 2^3 = 8$, soit $r' = 1$: le seul cas où x et y sont premiers entre eux est pour $x = 24$ et $y = 7$.

En prenant deux nombres premiers avec une puissance maximale, comme $5^2 \times 13$ ou $5^2 \times 17 < 1000$, on a $R = 24$ et $R' = 3$. Par exemple pour $325 = 5^2 \times 13$, on trouve $18^2 + 1^2$ ou $17^2 + 6^2$ ou $15^2 + 10^2$. On a aussi $r = 2^4 = 16$, $r' = 2$, avec (18, 1) et (17,6) premiers entre eux.

Pour $n < 2000$, on peut aller plus loin et prendre $5^3 \times 13 < 2000$ d'où $R = 32$ et $R' = 4$. On a en effet $1625 = 5^3 \times 13$ qui s'écrit $40^2 + 5^2$ ou $37^2 + 16^2$ ou $35^2 + 20^2$ ou $29^2 + 28^2$. On a encore $r = 16$ et $r' = 2$, soit deux cas où x et y sont premiers entre eux, comme on peut le vérifier.

En prenant trois nombres premiers distincts, qui ne peuvent être qu'à une puissance 1, on n'a jamais $n < 1000$. Mais on peut avoir $n < 2000$, notamment $5 \times 13 \times 17 = 1105$ et l'on trouve $R = 32$, d'où $R' = 4$. Précisément $1105 = 5 \times 13 \times 17 = 33^2 + 4^2$ ou $32^2 + 9^2$ ou $31^2 + 12^2$ ou $24^2 + 23^2$. Par la même occasion r est aussi maximal, soit $2^{3+2} = 32$. Les nombres x et y sont tous premiers entre eux.

Finalement la valeur maximale de R pour $n < 1000$ est 24, et elle vaut 32 pour $n < 2000$.

Exercice 2 : *Quel est le plus petit nombre n qui s'écrit de trois façons sous la forme $x^2 + y^2$ avec $x \geq y \geq 0$?*

Un nombre s'écrit de trois façons si $R' = 3$, soit $R = 24$ ou $R = 20$. Sous cette condition :

* Le plus petit nombre qui s'écrit sous forme d'une puissance d'un seul nombre premier est $5^4 = 625$ avec $R = 20$.
* Le plus petit nombre qui s'écrit avec deux nombres premiers dont l'un à la puissance 2 est $5^2 \times 13 = 325$ avec $R = 24$.
* Le plus petit nombre qui s'écrit avec trois nombres premiers tous à la puissance 1 est $5 \times 13 \times 17 = 1105$.

Finalement le plus petit nombre cherché est $n = 325$. On trouve $325 = 18^2 + 1^2$ ou $17^2 + 6^2$ ou $15^2 + 10^2$. On a aussi $r = 16$ et $r' = 2$, avec deux couples sur trois qui sont premiers entre eux.

Exercice 3 : *Trouver tous les nombres n inférieurs à 200 qui s'écrivent de deux façons comme somme de deux carrés.*

Supposons d'abord les nombres n impairs. Ceux qui s'écrivent de deux façons sont :

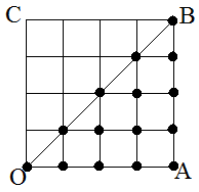
* les puissances (avec un exposant supérieur à 1) d'un nombre premier de la forme $4k + 1$. Pour $n < 100$, on trouve : $5^2 = 25$, $5^3 = 125$, $13^2 = 169$.
* les nombres formés de deux nombres premiers distincts : $5 \times 13 = 65$, $5 \times 17 = 85$, $5 \times 29 = 145$, $5 \times 37 = 185$.

Supposons maintenant les nombres n pairs. Il s'agit des nombres précédents multipliés par une puissance de 2. On trouve : $2 \times 25 = 50$, $4 \times 25 = 100$, $2 \times 65 = 130$, $2 \times 85 = 170$.

Finalement, il existe onze nombres inférieurs à 200 qui s'écrivent de deux façons, soit dans l'ordre : 25, 50, 65, 85, 100, 125, 130, 145, 169, 170, 185.

Exercice 4 *: Distances distinctes dans un réseau carré de $n \times n$ points*

1) On appelle g(n) le nombre de distances qui sont distinctes entre deux points quelconques du résea carré de $n \times n$ points. Calculer g(2) et g(3).

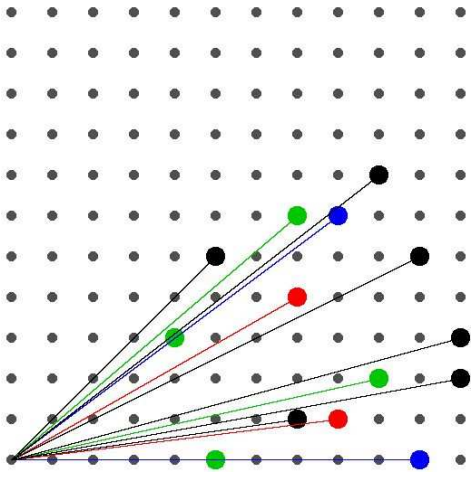


Les points du réseau carré de $n \times n$ points sont dans un carré $OABC$ de côté de longueur $n - 1$. Les distances d entre deux points quelconques sont au nombre de $\binom{n^2}{2}$ mais on s'intéresse seulement à celles qui sont distinctes. Pour des raisons de symétrie, on peut se contenter de les chercher dans le triangle OAB (en comptant les frontières). On peut aussi se contenter de chercher les distances distinctes d à partir du point O.

Dans le carré de côté 1, on trouve aussitôt $g(2) = 2$, soit $d^2 = 1$ ou $d^2 = 2$. Lorsque l'on passe à $n = 3$, il suffit d'ajouter une colonne de trois points au triangle précédent, et l'on a $g(3) = g(2) + 3 = 5$.

2) Constater qu'à partir de $n = 3$, on a d'abord $g(n) > n^2/2$, et trouver pour quelle valeur de n on a pour la première fois $g(n) < [n^2/2]$.

Procédons par récurrence. Pour passer du côté de longueur $n - 1$ à celui de longueur n, on ajoute une colonne de $n + 1$ points d'abscisse n, ce qui ajoute $n + 1$ nouvelles distances, d'où $g(n+1) = g(n) + n + 1$. Avec $g(2) = 2$, on a $g(3) = g(2) + 3$, $g(4) = g(3) + 4$, etc., on obtient la formule explicite $g(n) = n(n + 1) / 2 - 1$. Mais lorsqu'on ajoute les nouvelles distances à chaque étape, il peut arriver que l'on retrouve une ancienne distance, lorsque $d^2 = x^2 + y^2$ a deux solutions (x, y) $(x \geq y \geq 0)$. Les résultats obtenus dans l'*exercice 3* permettent de calculer les premiers $g(n)$:



$g(3) = 5$
$g(4) = 5 + 4 = 9$
$g(5) = 9 + 5 = 14$
$g(6) = 14 + 6 - 1 = 19$ à cause de $d^2 = 25$
$g(7) = 19 + 7 = 26$
$g(8) = 26 + 8 - 1 = 33$ à cause de $d^2 = 50$
$g(9) = 33 + 9 - 1 = 41$ à cause de $d^2 = 65$
$g(10) = 41 + 10 - 1 = 50$ à cause de $d^2 = 85$
De $n = 3$ à $n = 9$ on trouve que $g(n) > n^2/2$. Pour $n = 10$ on a $g(n) = n^2/2$.
$g(11) = 50 + 11 - 1 = 60$ à cause de $d^2 = 100$
Pour la première fois, avec $n = 11$, on a $g(n) < n^2/2$ et $g(n) = [n^2/2]$.
$g(12) = 60 + 12 - 2 = 70$, à cause de $d^2 = 125$ et $d^2 = 130$. Pour la première fois, avec $n = 12$ on a $g(n) < [n^2/2]$.

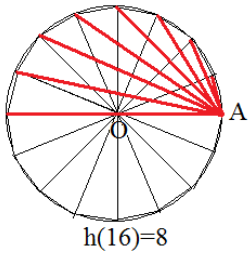
La figure ci-dessus fait ressortir les distances deux à deux égales dans le triangle OAB pour $n = 12$.

On a ensuite $g(13) = 82$, $g(14) = 93$, etc. Si l'on admet qu'il y a dorénavant toujours au moins une distance présente deux fois dans chaque nouvelle colonne, on a toujours $g(n) < [n^2/2]$, et comme le nombre de distances présentes deux fois (puis trois fois ...) a tendance à augmenter, la différence $n^2/2 - g(n)$ a aussi tendance à augmenter.

Remarque : Entre les réseaux carrés à n^2 et $(n+1)^2$ on peut prendre les cas intermédiaires avec n^2+1, n^2+2, etc. points. Appelons $g_1(N)$ le nombre des distances distinctes. On sait par exemple que $g_1(9) = 5$ et $g_1(16) = 9$. Dans les cas intermédiaires, on a $g_1(10) = g_1(11) = 6$, $g_1(12) = g_1(13) = 7$, $g_1(14) = g_1(15) = 8$. La fonction g_1 est croissante.

Un problème ouvert : *Parmi toutes les configurations de N points dans le plan, on désire trouver celle(s) dont le nombre des distances entre deux points quelconques est minimale. On appelle f(N) le nombre minimal des distances distinctes parmi toutes les configurations de N points.*

On a évidemment $f(2) = 1$, $f(3) = 1$ grâce à la configuration triangle équilatéral, $f(4) = 2$ grâce au carré, $f(5) = 2$ grâce au pentagone régulier. A défaut de trouver mieux, il semble que les polygones réguliers à N côtés correspondent aux configurations minimales. Appelons $h(N)$ le nombre de distances distinctes pour un polygone régulier à N sommets, et montrons que $h(N) = [N/2]$.



En effet, un polygone régulier a ses côtés égaux, et à partir d'un sommet il existe $N - 3$ diagonales. Si N est impair, le nombre des diagonales est pair, et par symétries, elles ont même longueur deux à deux, d'où $h(N) = 1 + (N-3)/2 = (N-1)/2 = [N/2]$. Si N est pair, il y a une diagonale qui est un diamètre, et les autres qui ont même longueur deux à deux, d'où $(N-4)/2 + 1 = (N-2)/2$ diagonales de longueur différentes[3], et $h(N) = N/2 = [N/2]$.

Mais si la formule $f(N) = h(N)$ reste valable pour les petites valeurs de N, on a vu que pour $N = 12^2 = 144$ (*cf. exercice 4*), la configuration du réseau carré donnait un nombre de distances distinctes $g(12) < [144/2]$. Il existe donc une valeur n_0 pour laquelle pour la première fois on n'a plus $f(N) = [N/2]$ mais une valeur inférieure $f(n_0) < [n_0/2]$, et $n_0 \leq 144$.

Algorithme donnant les solutions de $x^2 + y^2 = n$

Il s'agit, pour n donné, de trouver tous les x et y (avec $x \geq y \geq 0$) vérifiant $x^2 + y^2 = n$. La méthode que je développe ici s'apparente au tracé d'un cercle sur l'écran d'un ordinateur. Nous allons séparer les cas où n est impair et ceux où n est pair.

- **Cas où *n* est impair**

On sait déjà que si n est de la forme $4m + 3$, il n'existe aucune solution. Le seul cas à tratier est celui où n est de la forme $n = 1$ [4]. Procédons par étapes.

* Si l'équation $x^2 + y^2 = 4m + 1$ admet une solution, x et y sont forcément de parité différente, car s'ils avaient même parité, il en serait de même pour x^2 et y^2, et leur somme serait paire.

* Cela nous amène à réduire notre étude aux points (x, y) avec x et y de parité différente, situés dans le huitième de plan délimité par l'axe des x et la première diagonale du repère. Sur cette diagonale, aucun point ne nous intéresse puisque x et y ont alors la même parité. Pour des raisons de symétrie, tout point (x, y) de ce huitième de plan, et qui serait solution de $x^2 + y^2 = 4m + 1$, se trouvera répété huit fois dans le plan s'il n'est pas sur l'axe des x. S'il est sur l'axe des x, ou sur la première bissectrice du repère, il sera répété 4 fois.

* Pour éviter de devoir prendre un point sur deux dans le repère actuel, nous allons considérer un nouveau quadrillage du plan. Prenons un nouveau repère avec les axes $O'X$ et $O'Y$ tournés de 45° par

[3] Comme on le voit sur le dessin où tout se passe dans le demi-cercle supérieur, les distances *en rouge* ont toutes une longueur différente. Car si l'on prend deux des sommets *rouges P* et *P'*, le triangle *OPP'* est isocèle, et le seul triangle isocèle de sommets *P* et *P'* ayant son troisième sommet sur le cercle est tel que ce sommet est sur la médiatrice de [*PP'*] et donc situé sur le demi-cercle inférieur.

rapport aux anciens (on a aussi changé le sens, en prenant un angle de $-\pi/2$ entre ces axes. Le point *O'* est le point de coordonnées (1, 0) dans le repère initial. Les graduations du nouveau repère soit $\sqrt{2}$ fois celles de l'ancien. La formule de passage entre l'ancien et le nouveau quadrillage, pour un point *M* (*x*, *y*) ou (*X*, *Y*) est :

$$\begin{cases} x = X + Y + 1 \\ y = X - Y \end{cases}$$

Il y a bijection entre les points à coordonnées *x*, *y* de parité différente dans l'ancien repère du plan, et les points à coordonnées *X*, *Y* dans le nouveau repère du plan (*figure 1*).

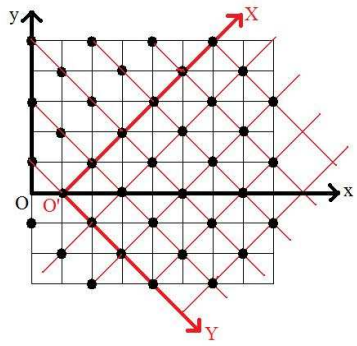


Figure 1 : Ancien et nouveau repère

* Plaçons-nous sur l'axe des *X*, et pour chaque point à coordonnées entières à partir de *O'*(1,0), considérons la suite *Z*(*X*, 0) des valeurs prises par $x^2 + y^2$. Au point (1,0) correspond la valeur Z(0, 0) = 1. Le point (1, 0) dans le nouveau repère ou (2, 1) dans l'ancien donne $Z(1, 0) = 2^2 + 1^2 = 5$, etc. On vérifie aisément que :

$Z(X, 0) = Z(X - 1, 0) + 4X$, [4] où *Z*(*X*, 0) est la valeur de $x^2 + y^2$ au point de coordonnées *X*, 0 dans le nouveau repère.

Si l'on se place maintenant sur l'axe des *Y*, on obtient par un calcul analogue :

$Z(0, Y) = Z(0, Y - 1) + 4\,Y$ [5]

* Prenons un point quelconque *M* (*x*, *y*) du quadrillage initial, ayant pour valeur $x^2 + y^2$. Dans le nouveau repère, ce même point *M* de coordonnées *X*, *Y* a pour valeur :

$Z(X, Y) = x^2 + y^2 = (X + Y + 1)^2 + (X - Y)^2 = 2X^2 + 2Y^2 + 2X + 2Y + 1$
avec aussi $Z(X, 0) = 2X^2 + 2X + 1$ et $Z(0, Y) = 2Y^2 + 2Y + 1$, d'où
$Z(X, Y) = Z(X, 0) + Z(0, Y) - 1$.

La valeur *Z* au point (*X*, *Y*) est égale à la somme des valeurs des projections du point sur les axes *O'X* et *O'Y*, diminuée de 1.

* Lien avec les nombres triangulaires. Sur l'axe *O'X*, on a trouvé la relation de récurrence *Z*(*X*, 0) = *Z*(*X* – 1, 0) + 4*X*, ce qui donne comme formule explicite

[4] Lorsque l'on passe d'un point (*x*, *y*) au point suivant (*x* + 1, *y* + 1) sur la diagonale, la valeur $x^2 + y^2$ passe à $(x + 1)^2 + (y + 1)^2$, soit une variation de 2*x* + 2*y* + 2. Le point initial *O*'(1, 0) ayant pour valeur *Z*(0, 0) = 1, on a une variation de valeur *Z*(1, 0) – *Z*(0, 0) = 4 d'après la formule précédente avec *x* = 1 et *y* = 0, et le point suivant a pour valeur *Z*(1, 0) = 1 + 4 = 5. On constate alors que la variation de la variation d'un point au suivant est égale à 4, puisque *x* augmente de 1 et *y* aussi. La variation *Z*(2, 0) – *Z*(1, 0) est donc 4 + 4 = 8, puis *Z*(3, 0) – *Z*(2, 0) = 8 + 4 = 12, d'où par récurrence, *Z*(*X*, 0) – *Z*(*X* – 1, 0) = 4 *X*.

[5] La variation d'un point au suivant est maintenant 2*x* – 2y + 2, d'où une première variation égale à 4, puis une variation de variation toujours égale à 4.

$Z(X, 0) = 1 + 4 + 8 + 12 + \ldots + 4X = 1 + 4\,X(X + 1)/2 = 1 + 4T_X$, en posant
$T_X = X(X + 1)/2$, T_X étant par définition le nombre triangulaire associé à X.
On a de même sur l'axe des Y : $Z(0, Y) = 1 + 4T_Y$ avec $T_Y = Y(Y + 1)/2$.

Pour un point quelconque du quadrillage, la relation $Z(X, Y) = Z(X, 0) + Z(0, Y) – 1$ devient : $Z(X, Y) = 4T_X + 4T_Y + 1$.

* Revenons à notre problème initial, où il s'agit de résoudre $x^2 + y^2 = n$ avec $n = 4m + 1$. En se plaçant dans le nouveau repère, cela devient $Z(X, Y) = 4m + 1$, et grâce à la formule précédente il reste : $T_X + T_Y = m$. D'où la propriété:

Résoudre $x^2 + y^2 = n$ avec $n = 4m + 1$ revient à résoudre $T_X + T_Y = m$ avec $x = X + Y + 1$ et $y = X – Y$.

Sur la *figure 2 à gauche* les points (x, y) de parité différente sont coloriés en fonction de la valeur de $n = x^2 + y^2$, plus précisément suivant la valeur de $m = (n – 1)/4$, et même de m ramené modulo 25, car on a utilisé une palette cyclique de 25 couleurs. Pour cette raison, le même motif se répète périodiquement dans le plan. *A droite*, les points (X, Y) dans le nouveau repère sont coloriés suivant la valeur de m en ces points, en utilisant la même palette cyclique de 25 couleurs. On peut constater l'identité de ces deux dessins, avec comme seule différence le fait que la figure de droite ne présente aucun trou.

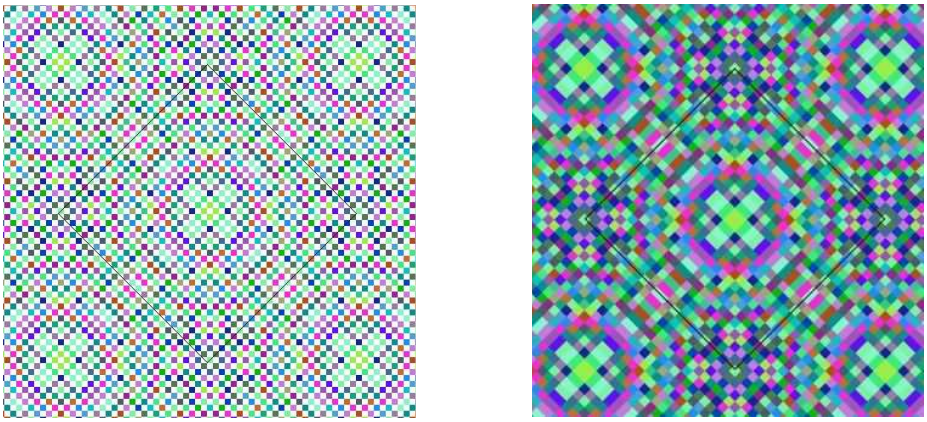


Figure 2 : *A gauche* points de parité différente (x, y) coloriés suivant la valeur de m avec $x^2 + y^2 = 4m + 1$, *à droite*, points (X, Y) coloriés suivant la valeur de m

Cette propriété va nous donner un algorithme simple et performant sur ordinateur pour trouver les solutions x, y de l'équation $x^2 + y^2 = 4m + 1$.

Algorithme de recherche des solutions de $T_X + T_Y = m$

Rappelons qu'il suffit de chercher les solutions de $x^2 + y^2 = n$ dans un huitième du plan, en cherchant les points à coordonnées entières sur le huitième de cercle (de centre O et de rayon $\sqrt{n}$) correspondant à cette équation. Pour cela nous allons utiliser un chemin oscillant au plus près autour de ce morceau de cercle (*figure 3 à gauche*). En fait, cela va être fait dans le nouveau repère $O'XY$, mais en le tournant de 45°, de façon que l'axe $O'X$ soit horizontal, et l'axe $O'y$ vertical. Le chemin oscillant autour du cercle se fait en marche d'escalier avec des marches verticales ou horizontales (*figure 3 à droite*). Le fait que le morceau de cercle concerné soit situé dans le huitième de plan tel que $X \geq Y$ impose que chaque marche horizontale a toujours une longueur unité.

Prenons l'exemple $m = 100$, ce qui est un cas favorable puisque $n = 401$ est un nombre de la forme $n = 1$ [4]. Commençons par déterminer un point d'ancrage : cherchons d'abord le plus petit X tel que

$T_X >$ 100. Ici il s'agit de $T_{14} = 105$. Diminuons X de 1, ce qui donne maintenant $T_x \leq 100$ (ici $T_{13} = 91$ différent de 100, donc pas de solution pour le moment). C'est le point de départ du chemin oscillant,

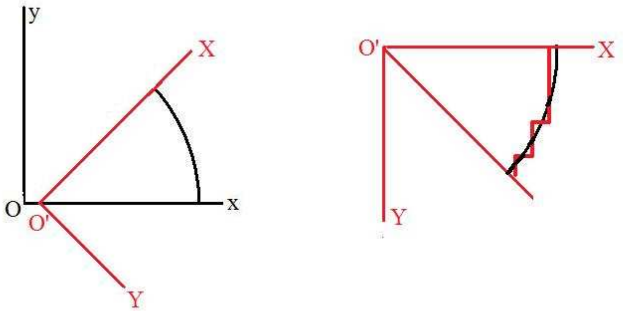


Figure 3 : *A gauche* le morceau de cercle sur lequel se trouvent les solutions entières de $x^2 + y^2 = n$, *à droite*, le même dessin dans le nouveau repère $O'XY$, en prenant maintenant l'axe $O'X$ horizontal et l'axe $O'y$ vertical, avec un chemin en marche d'escalier oscillant autour du cercle.

situé à gauche du cercle. Puis on entre dans une boucle répétitive tant que $X \geq Y$, où le point X, Y va décrire un chemin en marche d'escalier [6] (*figure 4*).

Partant du point ($X = 13$, $Y = 0$), faisons croître Y à partir de 0, et cherchons le plus petit Y tel que $T_X + T_Y \geq 100$. Ici il s'agit de $Y = 4$ avec T_4. On a $T_{13} + T_4 = 101 > 100$. On est maintenant à droite du cercle, toujours au plus près. Au cas où l'on aurait eu $T_X + T_Y = 100$, on afficherait le résultat, mais ce n'est pas le cas ici. Signalons que le calcul des nombres triangulaires se fait uniquement par addition, en utilisant la récurrence $T_k = T_{k-1} + k$. A partir du point (13, 4), on diminue maintenant X de 1, d'où le point (12, 4) situé à gauche du cercle. On est alors sûr que $T_{12} + T_4 < 100$ ($T_{12} + T_4 = 101 - 13 = 88$). On augmente ensuite Y jusqu'à ce que $T_X + T_Y \geq 100$. Si l'on tombe sur une égalité, on affiche le résultat. Ici on trouve que l'on arrive au point (12, 7) avec $T_{12} + T_7 = 106$. On continue en diminuant X de 1 : $T_{11} + T_7 = 106 - 12 = 94 < 100$ au point (11, 7). Ensuite on augmente Y jusqu'au point (11, 8) tel que $T_{11} + T_8 = 94 + 8 = 102$. On diminue X de 1, en passant au point (10, 8) avec $T_{10} + T_8 = 102 - 11 = 91 < 100$, puis en augmentant Y, jusqu'au point (10, 9) avec $T_{10} + T_9 = 91 + 9 = 100$, qui est la première solution trouvée. On continue ainsi tant que $X \geq Y$, ce qui donnera toutes les solutions. Dans le cas présent, cette solution est unique, car le nombre $n = 401$ est un nombre premier.

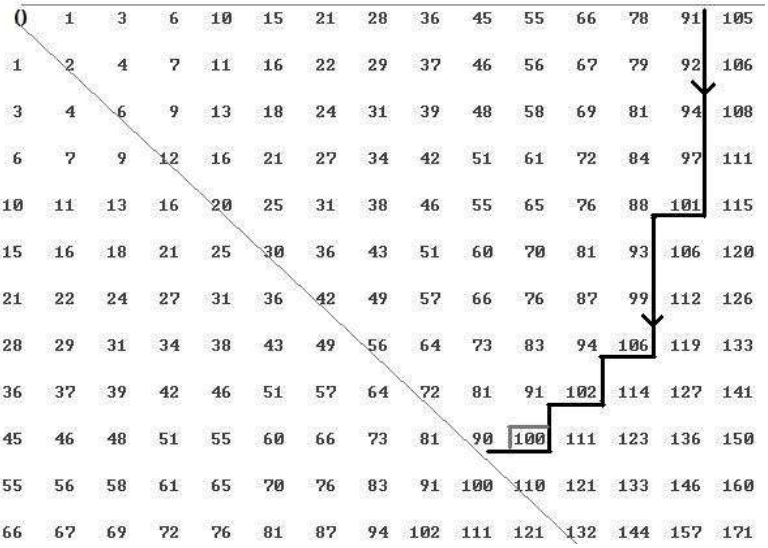


Figure 4 : Chemin oscillant au plus près autour d'un arc de cercle

[6] On est toujours au plus près de $T_X + T_Y = 100$, soit $X^2 + Y^2 + X + Y = 200$, ce qui donne un arc de cercle de centre (–1/2, –1/2) qui n'est autre que l'origine du repère initial O, et de rayon R tel que $R^2 = 200{,}5$, ou encore $R^2 = 401$ en prenant les unités du repère initial.

On repasse enfin au problème initial en faisant $n = 4m + 1$. Ici, la seule solution trouvée correspondant à $T_{10} + T_9 = 100$, donne dans le repère initial, en utilisant la formule de changement de repère : $20^2 + 1^2 = 401$. Cela fait finalement huit solutions par symétries. De cet exemple découle l'algorithme général.

Comme exemple d'application, pour $n = 48\ 612\ 265$ (de la forme $4m + 1$), les solutions (x, y) positives et dans l'ordre $x \geq y$ sont :

```
solution  1 :  5008  4851
solution  2 :  5139  4712
solution  3 :  5179  4668
solution  4 :  5243  4596
solution  5 :  5432  4371
solution  6 :  5613  4136
solution  7 :  5656  4077
solution  8 :  5691  4028
solution  9 :  5832  3821
solution 10 :  5907  3704
solution 11 :  6048  3469
solution 12 :  6124  3333
solution 13 :  6213  3164
solution 14 :  6259  3072
solution 15 :  6384  2803
solution 16 :  6404  2757
solution 17 :  6413  2736
solution 18 :  6556  2373
solution 19 :  6576  2317
solution 20 :  6637  2136
solution 21 :  6651  2092
solution 22 :  6756  1723
solution 23 :  6772  1659
solution 24 :  6789  1588
solution 25 :  6853  1284
solution 26 :  6899  1008
solution 27 :  6917  876
solution 28 :  6944  627
solution 29 :  6948  581
solution 30 :  6952  531
solution 31 :  6971  132
solution 32 :  6972  59
```

- **Cas où *n* est un nombre pair**

* Jusqu'à présent nous avions supposé n impair de la forme $n = 4m + 1$. Plaçons-nous maintenant dans le cas où $n = 2^d (4m + 1)$, avec $d > 0$. Si l'on avait $n = 2^d (4m + 3)$ il n'y aurait toujours aucune solution.

* Supposons d'abord que $d = 1$, soit $n = 2(4m + 1)$. Rappelons qu'on sait traiter $x^2 + y^2 = 4m + 1$ par le biais de $T_X + T_Y = m$, permettant d'avoir les solutions (X, Y) correspondantes. Cette dernière équation s'écrit aussi :

$X(X + 1)/2 + Y(Y + 1)/2 = m$, ou $X^2 + Y^2 + X + Y = 2m$,
ou encore $(X + 1/2)^2 + (Y + 1/2)^2 - 1/2 = 2m$, soit
$(2X + 1)^2 + (2Y + 1)^2 = 2\ (4m + 1)$.

Connaissant X et Y, on vient de trouver $X' = 2X + 1$ et $Y' = 2Y + 1$ qui vérifient $X'^2 + Y'^2 = n$. Et comme il y a toujours autant de solutions, on les a toutes.

* Exemple : $n = 338 = 2 \times 169 = 2(4 \times 42 + 1)$, avec $m = 42$. On commence par résoudre $T_X + T_Y = 42$ par l'algorithme précédent, ce qui donne $T_8 + T_3 = 42$ et $T_6 + T_6 = 42$ comme seules solutions avec $X \geq Y \geq 0$, ou encore $12^2 + 5^2 = 169$, $13^2 + 0^2 = 169$. Par symétries on trouve $8 + 4 = 12$ solutions pour $x^2 + y^2 = 169$. On en déduit $17^2 + 7^2 = 338$ et $13^2 + 13^2 = 338$, d'où les 12 solutions de $X'^2 + Y'^2 = 338$.

* Supposons maintenant que *d* est un nombre pair : $d = 2d'$, d'où $n = 2^{2d'}(4m + 1)$. Pour avoir les solutions de $x^2 + y^2 = n$, il suffit de prendre les solutions de $x^2 + y^2 = 4m + 1$ puis de les multiplier par $2^{d'}$, ce qui donne toutes les solutions.

* D'où le complément d'algorithme lorsque *n* est pair :

a) Si *d* est pair ($d = 2d'$), avec $n = 2^d (4m + 1)$, on détermine toutes les solutions pour $4m + 1$ et on les multiplie par $2^{d'}$.

b) Si *d* est impair ($d = 2d' + 1$), avec $n = 2^d (4m + 1)$, on détermine toutes les solutions de $T_X + T_Y = m$, on en déduit les solutions de $X'^2 + Y'^2 = 2(4m + 1)$ par $X' = 2X + 1$ et $Y' = 2y + 1$, puis l'on multiplie ces solutions par $2^{d'}$ pour avoir toutes les solutions de $x^2 + y^2 = n$.

On en déduit le programme complet :

```
main()
{
Se donner n et mettre compteur à 0 (compteur va donner le nombre de solutions)
nn=n ; d=0 ;   while(nn%2==0) { nn=nn/2 ; d++;}
if (d%2==0)  dd = d/2 ;     else dd = (d-1)/2 ;    deuxpdd=pow(2.,dd);
m=(nn-1)/4;     if ( (nn-1)%4!=0) { printf("Aucune solution"); getchar(); exit(0);}
TX=0; X=0; TY=0; Y=0;       while(TX<m)  { X++ ;  TX + =X ; }
if (TX==m)    { compteur++;    afficher le résultat   }
delta= TX-m;
for(;;)
  {do  { delta -=X ;   X-- ;
           while(delta<0  && X>Y)  { Y++; TY+=Y; delta+=Y; }
         }
    while(delta!=0 && X>=Y);
    if (delta==0)   { compteur++;  afficher le résultat   }
    if (X<=Y) break;
  }
}
```

Afficher le résultat consiste à faire:

```
if (d%2==0)
printf("%ld:(%ld %ld) ",compteur, deuxpdd*(X+Y+1), deuxpdd*(X-Y));
else   printf("%ld:(%ld %ld) ",compteur, deuxpdd*(2*X+1), deuxpdd*(2*Y+1));
```