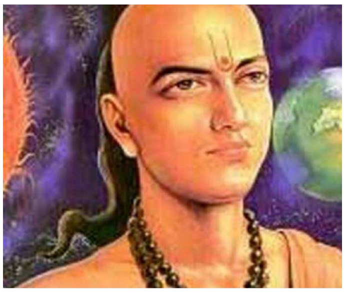
MATHEMATIQUES DE L'INDE ANCIENNE des années 500 à 1600

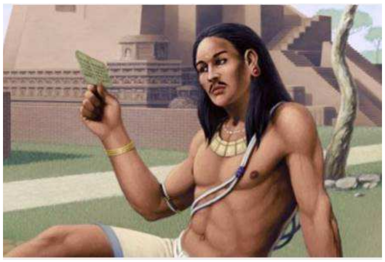
L'âge d'or des mathématiques de l'Inde ancienne[1] se situe en gros entre les années 500 et 1600. Notre étude se réduira à cette période particulièrement faste, et se concentrera sur la combinatoire, sur l'arithmétique et sur les suites et séries.

1. Quelques grands mathématiciens de la période classique

 Aryabhata

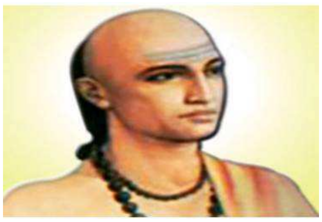
Aryabhata, années 500, le précurseur des mathématiques indiennes. Dans les siècles qui suivent, 18 commentaires sont faits sur son oeuvre, l'*Aryabhatiya*.

Bhaskhara I (600-680). En 629, il écrit des commentaires sur l'*Aryabhatiya*

 Brahmagupta

Brahmagupta (598-670)

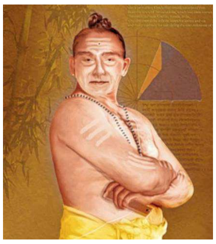
Sridhara (autour du 9è siècle)
Mahavira (années 800)

 Bhaskara II

Bhaskhara II (1114-1185)

Narayana Pandita (1340-1400)

[1] Dans un premier temps, j'avais titré ce document « mathématiques indiennes « . C'eût été faire preuve de malhonneteté intellectuelle. Car l'Inde ancienne, c'est non seulement l'Inde d'aujourdhui, mais tout autant le Pakistan, le Bengladesh, le Népal, voire une partie de l'Afghanistan. Cela n'empêche pas l'historien indien G.G. Joseph d'intituler son dernier livre, par ailleurs très intéressant, « *Indian Mathematics* ». Il se prête ainsi à la critique faite par Al-Biruni dans les années 1000, à propos de ses collègues mathématiciens indiens : ceux-ci ont tendance à considérer qu'« il n'est de mathématiques que la leur ». Peut-être faut-il voir là l'influence du système hiérarchique des castes, avec en dessous d'elles les intouchables.


Madhava de Sangamagramma

Madhava de Sangamagramma (1340-1425) fonde l'école de mathématiques et d'astronomie du Kerala.
Nilakantha Somayagi, (1444-1544), le plus connu des mathématiciens de l'Ecole de Kerala.

Seuls Sridhara et Mahavira sont exclusivement mathématiciens, les autres sont aussi astronomes.

Al Biruni

Citons enfin **Al Biruni** (973-1048), originaire de l'actuel Ouzbékistan. Fait prisonnier par le sultan Mahmud de Ghazni (en Afghanistan) lorsque celui-ci mène sa première expédition militaire jusqu'en Inde (il en fera 17), il devient vite une autorité du régime, et réside de longues années en Inde. Al Biruni est un savant encyclopédiste, lisant aussi bien bien les textes grecs que ceux en sanskrit. Il a non seulement concentré les connaissances venant de larges horizons, mais les a aussi transmises de l'est vers l'ouest et de l'ouest vers l'est.[2] Il traduit notamment les textes d'Euclide et de Ptolémée en sanskrit. Son profond intérêt pour la culture indienne ne va pas sans certaines réticences. Il estime que la littérature mathématique et astornomique indienne est un « mélange de pierres précieuses et de verroterie ».[3] Voici une anecdote à son sujet :

Le sultan Masud, fils de Mahmud, offre au savant Al Biruni le poids d'un éléphant en pièces d'argent. Celui-ci décline le cadeau : « Ce présent m'éloignerait de la science. Jamais je ne troquerai la pérennité de mon savoir scientifique contre l'éclat éphémère du clinquant, car les sages savent que l'argent passe vite, tandis que la science reste ».

Le manuscrit Bakhshali, découvert en 1881 près de Peshawar (Pakistan actuel), est le plus ancien document existant ayant trait aux mathématiques indiennes. Il comprend 70 feuilles à base d'écorce de bouleau. Sa date est incertaine, entre le 9è siècle et le 12è selon certains, mais en analysant son contenu, il pourrait être la copie d'un manuscrit plus ancien datant du 3è ou 4è siècle. D'ailleurs certains historiens indiens le datant même des années 600, voire des années 200.

La transmission du savoir mathématique se fait beaucoup par voie orale. Certains textes sont écrits en sanskrit, et constitués de *sutras* en vers, très hermétiques à cause de la compression de leur formulation. Cela permet aux disciples des maîtres de les apprendre par coeur, de génération en génération. D'autres mathématiciens se chargent plus tard de les développer pour les rendre plus compréhensibles, en les illustrant par de nombreux exemples. Pour cette raison, de nombreux textes mathématiques indiens sont appelés « commentaires » d'oeuvres plus anciennes. Mais il existe aussi une transmission par écrit, utilisant essentiellement des feuilles de palmier, qui sont d'abord imperméabilisées. Puis les textes y sont gravés avec une aiguille, les rainures étant enfin remplies avec de l'encre ou des pigments.

Dans ce qui suit, nous n'abordons que certains aspects des mathématiques, ceux qui nous ont semblé les plus originaux. Nous n'aborderons pas les problèmes de géométrie-astronomie, ni les problèmes classiques de calcul. Signalons toutefois que les problèmes posés sont souvent imagés et pleins de fantaisie, de façon à captiver l'attention du lecteur.

Comme ce problème posé par Sridhara : « *Durant une querelle d'amoureux, un collier est brisé, avec un tiers des perles qui restent éparpillées par terre, un cinquième qui tombe sur le lit, un sixième qui est ramassé par une servante, et un dixième ramassé par l'amant. Six perles restent sur le collier. Combien le collier avait-il de perles ?* » (la réponse est 30).

Ce problème est repris par Mahavira : « *Par une nuit de printemps, une jeune femme est amoureusement blottie contre son mari dans une grande maison blanche comme la lune, entourée d'un jardin rempli d'arbres gorgés de fruits et de fleurs.*

[2] cf. *le Courrier de l'Unesco* 6- 1974, numéro spécial consacré à Al Biruni.

[3] Cela lui est reproché de nos jours par l'historien indien G. G. Joseph [JOS2016], qui pense qu'Al Biruni n'a pas bien compris le sanskrit scientifique exprimé en vers.

Le lieu est bruissant des sons suaves des perroquets, des coucous et des abeilles enivrées de miel. Mais au cours d'une querelle amoureuse, le collier de la dame se détache et les perles s'éparpillent alentour. Un tiers est récupéré par la servante assise à proximité, un sixième tombe sur le matelas, la moité de ce qui reste, puis la moitié de ce qui reste après, et ainsi de suite six fois, restent éparpillés sur le sol. Sur le collier brisé ne restent que 1161 perles. Oh mon amour, dis-moi vite le nombre de perles du collier. » Le résultat, 148 608 perles, illustre la fantaisie du problème, loin de la froide logique mathématique, tout en montrant une certaine fascination pour les grands nombres.

2. Combinatoire

Dans les années -200, Pingala, considéré comme un théoricien de la musique, calcule le nombre de façons de mélanger deux types de sons, longs et courts, dans une composition poétique de trois sons, ce qui fait, en distinguant les cas : 1, 3, 3, 1. Plus tard, vers les années 1100, Halayudha commente les travaux de Pingala et explique comment écrire des lignes de nombres dans un triangle, correspondant à ce qu l'on appelle en France le triangle de Pascal, et il l'intitule « escalier du mont Meru », un mont mythique pour les Indiens, à l'image du mont Olympe pour les Grecs. Il s'agit là des premières notions de combinatoire, à base de linguistique mathématique. [4]

Mais le plus original est l'apparition de problèmes combinatoires liés à la vie courante. Dans un traité de médecine, progressivement élaboré entre les années -500 et 400, et attribué notamment à Sushruta, on trouve que l'on peut faire 63 combinaisons à partir de mélanges de six saveurs : l'amer, le salé, l'acide, le sucré, le piquant, l'astringent, en en prenant une, deux, trois, etc. Il s'agit en effet de

$C_6^1 + C_6^2 + C_6^3 + C_6^4 + C_6^5 + C_6^6 = 6 + 15 + 20 + 15 + 6 + 1.$

Dans les années 800, Sridhara traite le même exemple plus précisément et donne la formule générale des combinaisons $C_n^p = n\,(n-1)(n-2)...(n-p+1)/\,p\,!$.

Vers 1150, Bhaskara II pose cet exercice :

Un roi vit dans un splendide palais qui a 8 grandes portes construites par d'ingénieux ouvriers pour assurer la ventilation des pièces. Selon qu'elles sont ouvertes ou fermées, combien y a-t-il de types de ventilation possible ?

En ajoutant les nombres de combinaisons pour une porte ouverte, deux portes ouvertes, etc., il arrive au résultat de 255.[5] Il est sous-entendu que le cas où toutes les portes seraient fermées n'est pas pris en compte, puisqu'il n'y a alors aucune ventilation.

Il ressort de là que les savants indiens ont nettement insisté sur l'aspect dénombrement, apparemment plus que leurs homologues arabes ou plus tard européens qui eux, ont souvent privilégié l'aspect algébrique, les combinaisons devenant les coefficients binomiaux.

3. Au-delà des suites arithmétiques

Aryabhata traite les suites arithmétiques dans son texte *Aryabhatiya*. Selon les commentaires qu'en faits plus tard Bhaskara I, on aboutit notamment à ce genre de développements :

• Etant donnés le premier terme a de la suite, sa raison r, et la somme S de ses termes, trouver quel est le nombre n des termes. Il aboutit à la formule :

$$n = \frac{1}{2}\left(\frac{\sqrt{8rS + (2a-r)^2} - 2a}{r} + 1\right)$$

Bhaskara I prend l'exemple avec $a = 5$, $r = 7$ et $S = 95$, et il déduit de la formule $n = 5$. De son côté, Sridhara traite le cas avec $a = 20$, $r = 5$ et $S = 245$, ce qui donne $n = 7$. Cette formule sous-entend que la résolution d'une équation du second degré est bien connue.

• Bhaskara I démontre aussi la formule classique sur la somme des cubes :

$1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2$ grâce à une méthode originale :

$$\begin{aligned}1^3 + 2^3 + ... + n^3 &= 1 + (3 + 5) + (7 + 9 + 11) + ... \\ &\quad + ((1+ n(n-1)) + (3 + n(n-1)) + ... + (2n-1 + n(n-1)))\end{aligned}$$

---

[4] Dans l'*Atlas des mathématiques* (livre de poche 1997), on peut lire : « L'analyse combinatoire est née de l'étude des jeux de hasard ». Il est vraisemblable que les probabilités se sont forgées dans les temps très anciens à partir de divers jeux comme les osselets, mais cela n'a pas empêché la combinatoire de suivre une voie propre, indépendante du calcul de probabilités. Signalons que des problèmes de dénombrement liés à la linguistique apparaissent aussi, comme en Inde, en Chine et dans le monde arabo-musulman.

[5] Le résultat 255 est aussi $2^8 - 1$, ce - 1 provenant du fait que l'on ne compte pas le cas où il n'y a aucune ventilation.

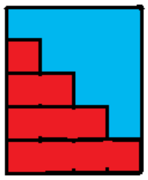
en utilisant la formule sur la somme des termes d'une suite arithmétique.[6]

Cela s'écrit donc $1^3 + 2^3 + ... + n^3 = 1 + 3 + 5 + 7 + 9 + 11 + ... + (n (n + 1) - 1)$. Sachant que la somme des N premiers nombres impairs est $1 + 3 + 5 + ... + (2N - 1) = N^2$, et que dans le cas présent, le nombre de termes est $N = 1 + 2 + 3 + ... + n = n (n + 1) / 2$, on trouve la formule cherchée.

3.1. Nombres triangulaires $T_n = 1 + 2 + 3 +...+ n$

Au 15è siècle, Narayana reprend les résultats sur les nombres triangulaires et les généralise. Il commence par donner une démonstration géométrique de la formule de base :

$$\sum_{k=1}^{n} k = T_n = \frac{n(n+1)}{2}$$



Pour ce faire, il prend le nombre $T_n = 1 + 2 + ... + n$, appelé nombre triangulaire de façon imagée, en le représentant par des barres posées l'une sur l'autre, dont la longueur augmente d'une unité de haut en bas. Sur la figure, la surface rouge représente $T_4 = 1 + 2 + 3 + 4$. En construisant le rectangle de base n et de hauteur $n + 1$, celui-ci englobe deux fois le nombre triangulaire T_n (en rouge et en bleu sur le dessin pour $n = 4$), d'où la formule $T_n = n (n + 1) / 2$. En faisant une lecture colonne par colonne, on retrouve la méthode de Gauss.[7]

Puis il procède à une généralisation de la formule :

$$\sum_{k=1}^{n} k = T_n = \frac{n(n+1)}{2}$$

$$\sum_{p=1}^{n}\sum_{k=1}^{p} k = \sum_{p=1}^{n} T_p = \sum_{p=1}^{n} \frac{p(p+1)}{2} = \frac{n(n+1)(n+2)}{2\times 3}$$

$$\sum\sum\sum k = \sum_{k=1}^{n} \frac{k(k+1)(k+2)}{2\times 3} = \frac{n(n+1)(n+2)(n+3)}{2\times 3\times 4}$$

$$\sum_{k=1}^{n} \frac{k(k+1)(k+2)(k+3)}{4!} = \frac{n(n+1)(n+2)(n+3)(n+4)}{5!} \qquad (n \geq 1)$$

etc.

Et pour illustrer l'utilité de ces formules, il pose un problème assez coriace, mine de rien.

Le problème de la vache

Une vache donne naissance à un veau chaque année. Chaque veau, après trois années, devient une vache donnant naissance à un veau chaque année. Combien a-t-on de vaches et de veaux au bout de 20 années ?

Les enfants de la vache sont au nombre de $V_{20}^{(1)} = 20$.

Les enfants des enfants de la vache sont au nombre de $V_{17}^{(2)} = T_{17} = \frac{17\times 18}{2}$

Les enfants des enfants des enfants sont au nombre de $V_{14}^{(3)} = \frac{14\times 15\times 16}{2\times 3}$

Et ainsi de suite :

$$V_{11}^{(4)} = \frac{11\times 12\times 13\times 14}{2\times 3\times 4}$$

$$V_{8}^{(5)} = \frac{8\times 9\times 10\times 11\times 12}{2\times 3\times 4\times 5}$$

$$V_{5}^{(6)} = \frac{5\times 6\times 7\times 8\times 9\times 10}{2\times 3\times 4\times 5\times 6}$$

$$V_{2}^{(7)} = \frac{2\times 3\times 4\times 5\times 6\times 7\times 8}{2\times 3\times 4\times 5\times 6\times 7}$$

Par addition des V, on trouve 2744. En ajoutant la vache initiale, cela fait 2745 vaches et veaux

---

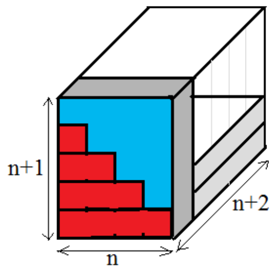
[6] En effet, le $p^{\text{ème}}$ terme, qui est lui-même formé d'une somme de p éléments est $u_0 + (u_0 + 2) + (u_0 + 4) + ... + (u_0 + 2 (p - 1))$ avec $u_0 = 1 + p (p - 1)$, et il vaut $p\, u_0 + p (p - 1) = p^3$ après simplification.

[7] Pour calculer $S = 1 + 2 + 3 +...+ 100$, K. F. Gauss avait utilisé l'écriture à l'envers $S = 100 + 99 + ... + 1$, et ajouté les deux égalités précédentes colonne par colonne pour trouver $2S = 100 \times 101$.

Un peu plus tard, c'est en utilisant ce même genre de barres que Nilakantha Somayagi fait la démonstratio de la formule : $\sum_{k=1}^{n} \frac{k(k+1)}{2} = \frac{n(n+1)(n+2)}{6}$, ou encore :
$1 \times 2 + 2 \times 3 + 3 \times 4 + ... + n\ (n+1) = n\ (n+1)\ (n+2) / 3$, ou encore

$3\ (1 \times 2 + 2 \times 3 + 3 \times 4 + ... + n\ (n+1)) = n\ (n+1)\ (n+2)$

Pour ce faire, il utilise des plaques de longueur $k + 1$, de largeur k et de hauteur 1, de volume $k\ (k + 1)$. Une telle plaque représente deux fois le nombre triangulaire T_k. Puis il prend le pavé dont les côtés mesurent n, $n + 1$ et $n + 2$.



Dans ce pavé, il commence par placer trois plaques $n \times (n+1)$, l'une verticale, et les deux autres posées sur le sol, comme indiqué sur le dessin pour $n = 4$. Cela étant fait, il reste à remplir un pavé de côtés $n - 1$, n et $n + 1$. Il suffit de refaire comme précédemment avec trois plaques $(n - 1) \times n$, pour se retrouver avec un pavé vide de volume $(n - 2)\ (n - 1)\ n$. Et ainsi de suite. A la fin du remplissage avec des plaques de plus en plus petites, on arrive à la formule cherchée.

Mais on ne peut plus utiliser le même genre d'arguments géométriques (il faudrait passer en 4 dimensions) pour démontrer la formule de l'étape suivante :

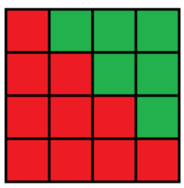
$\sum\sum\sum k = \sum_{k=1}^{n} \frac{k(k+1)(k+2)}{2 \times 3} = \frac{n(n+1)(n+2)(n+3)}{2 \times 3 \times 4}$. Celle-ci peut seulement être considérée comme le prolongement de la formule précédente.

Digression

Ce genre de méthode géométrique indienne, qui fut aussi utilisée par les grecs, les arabes et les chinois dans les temps anciens, donne plusieurs idées.

- *Comment obtenir la formule des carrés :* $1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$*, à partir de la formule sur la somme des nombres triangulaires ?*

Cette formule des carrés est bien connue, notamment de Narayana et de Nilakantha, mais je n'ai pas trouvé de démonstration qu'ils auraient pu faire de cette formule. En voici une, qui était tout à fait à leur portée :



En prenant un carré de n sur n, on constate aussitôt que $T_{n-1} + T_n = n^2$, comme sur la figure pour $n = 4$. On en déduit que :

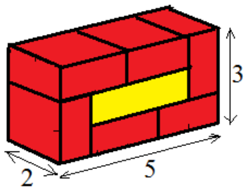
$$1^2 + 2^2 + 3^2 + ... + n^2 = T_1 + (T_1 + T_2) + (T_2 + T_3) + (T_3 + T_4) + ... + (T_{n-1} + T_n)$$
$$= 2\ (T_1 + T_2 + T_3 + ... + T_{n-1}) + T_n = 2 \frac{(n-1)\ n\ (n+1)}{6} + \frac{n(n+1)(n+2)}{6}$$
$$= \frac{n(n+1)(2n+1)}{6}$$

- *Comment obtenir la formule des carrés par une construction géométrique ?*

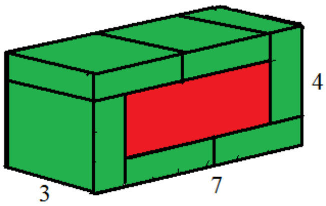
Nous la donnons ici sous forme de puzzle en trois dimensions, proche de la démonstration précédente de Nilakantha.

On dispose de plaques dont la base est carrée, et toutes de même épaisseur un. Plus précisément, on a six plaques de 1 sur 1 (des cubes) de couleur jaune, six plaques de 2 sur 2 de couleur rouge, six plaques de 3 sur 3 de couleur verte, et six plaques de 4 sur 4 de couleur bleue. En disposant judicieusement ces 24 plaques, construire un pavé rectangulaire sans qu'il n'y ait aucun trou, de façon que l'ensemble des faces (la surface extérieure) n'ait pas plus de deux couleurs présentes. Au cas où vous n'y arrivez pas, on peut vous préciser que ce pavé a pour dimensions $4 \times 5 \times 9$.

On aura intérêt à reconnaître la formule sur la somme des carrés, avec $n\ (n + 1)\ (2n + 1)$ pour $n = 4$. Dans ces conditions, commençons par construire un pavé de $1 \times 2 \times 3$ avec les six cubes dont nous disposons, en prenant 1 comme hauteur. Puis enrobons-le au moyen des six plaques de côté 2 comme indiqué sur le dessin.



Tournons ce pavé de façon qu'il ait pour hauteur 2, et enrobons-le en utilisant les six plaques de côté 3. On constate que deux couleurs sont présentes sur les faces du pavé.



Puis tournons ce pavé afin que sa hauteur soit 3, et enrobons-le comme précédemment avec les six plaques de 4 sur 4. On obtient bien le pavé de côtés $4 \times 5 \times 9$, avec deux couleurs présentes, verte et bleue.

On pourrait d'ailleurs continuer avec des plaques plus grandes, ce qui redémontre la formule sur la somme des carrés $1^2 + 2^2 + 3^2 + \ldots$

- *La méthode de Bhargava*

Nouveau rebondissement au sujet de la formule sur la somme des nombres triangulaires $\sum_{k=1}^{n} \frac{k(k+1)}{2} = \frac{n(n+1)(n+2)}{6}$, dans les années 1980, grâce au mathématicien canadien d'origine indienne M. Bhargava. A l'âge de 7 ans, il trouve une nouvelle démonstration géométrique de la formule. La somme des nombres en ligne : $1 + 2 + \ldots + k = k\,(k + 1) / 2$ peut être représentée par des étages de billes qui forment une pyramide à base triangulaire. En haut se trouve une bille, à l'étage au-dessous $3 = 1 + 2 = 2 \times 3 / 2$ billes, puis au-dessous $6 = 1 + 2 + 3 = 3 \times 4 / 2$ billes, etc. Cette somme de nombres triangulaires est d'ailleurs appelée nombre tétraédrique. Il s'agit de prouver que le nombre tétraédrique S_n vaut $n\,(n + 1)\,(n + 2) / 6$.

$$\begin{array}{c} \downarrow \\ 1 \\ 1\ 2 \\ 1\ 2\ 3 \\ 1\ 2\ 3\ 4 \\ \nearrow\ 1\ 2\ 3\ 4\ 5\ \nwarrow \end{array}$$

M. Bhargava fait trois lectures de cette somme, selon les trois flèches du dessin. Vu de haut, on obtient, étage par étage : $1 + (1 + 2) + (1 + 2 + 3) + \ldots + (1 + 2 + 3 + \ldots + n)$. De même en regardant à partir de la gauche. Mais en regardant à partir du côté droit, on a

$n + 2\,(n - 1) + 3\,(n - 2) + \ldots + n \times 1$

$$\begin{aligned} \text{Ainsi } 3\,S_n &= 1 + 1 \times 2/2 \quad + 2 \times 3/2 + \ldots \quad + n\,(n + 1)/2 \\ &\quad + 1 + 1 \times 2/2 \quad + 2 \times 3/2 + \ldots \quad + n(n+1)/2 \\ &\quad + n + 2\,(n - 1) + 3\,(n - 2) + \ldots + n \times 1 \end{aligned}$$

Le terme dans la colonne k (à partir de $k = 1$) s'écrit $k\,(k + 1) + k\,(n - k + 1) = k\,(n + 2)$. D'où :

$3\,S_n = (1 + 2 + 3 + \ldots + n)\,(n + 2) = n\,(n + 1)\,(n + 2) / 2$. C'est la formule cherchée.

3.2. Factorisation d'entiers

Même dans ce domaine vont réapparaître les suites arithmétiques.

A l'origine, Narayana s'était rendu compte qu'un nombre impair N s'écrit toujours comme une différence de deux carrés, ce qui permet une factorisation : $N = a^2 - b^2 = (a + b)(a - b)$. Il prend comme exemple $N = 1161$. Pour cela il commence par calculer $a_0 = [\sqrt{N}\,] = 34$. On a alors $r_0 = a_0^2 - N = 34^2 - 1161 = -5$. Il prend ensuite $a_1 = a_0 + 1 = 35$, avec $r_1 = (a_0 + 1)^2 - N = r_0 + 2a_0 + 1 = -5 + 69 = 64 = 8^2$. Finalement $35^2 - 1161 = 8^2$, $1161 = 35^2 - 8^2 = (35 + 8)(35 - 8) = 43 \times 27$.

Mais cela n'est pas toujours aussi simple. En règle générale, le calcul ne s'arrête pas dès a_1. Il convient de continuer en essayant $a_2 = a_0 + 2$, $a_3 = a_0 + 3$, etc. On avait vu que $r_1 = r_0 + u_0$ avec $u_0 = 2a + 1$. On constate que l'on a ensuite : $r_2 = r_0 + u_0 + 2$, puis $r_3 = r_0 + u_0 + (u_0 + 2) + (u_0 + 4)$, etc. D'où l'apparition d'une suite arithmétique de raison 2. On continue jusqu'à l'obtention d'un carré, soit $r_{p+1} = b^2$, avec $r_0 + u_0 + (u_0 + 2) + (u_0 + 4) + \ldots + (u_0 + 2p)$. Comme on a aussi : $r_{p+1} = (a_0 + p + 1)^2$, on trouve la factorisation $N = (a_0 + p + 1 + b)(a_0 + p + 1 - b)$.

G.G. Joseph [JOS2016] prend comme exemple $N = 1001$, mais avec une certaine ambiguité. On ne sait pas trop si c'est bel et bien un exemple dû à Narayana, ou une extrapolation de sa méthode utilisée pour $N = 1161$. Dans le premier cas, Narayana aurait découvert la méthode dite de Fermat 250 ans avant lui. Dans le deuxième cas, il n'aurait fait qu'entrevoir ce qui serait plus tard la méthode de factorisation de Fermat.

Traitons $N = 1001$. On trouve $a_0 = 31$, $r_0 = a_0^2 - N = -40$ et $u_0 = 2a_0 + 1 = 63$. Puis en ajoutant les termes successifs de la suite arithmétique, on constate que $-40 + 63 + 65 + 67 + 69 + ... + 89 = 1024 = 32^2$. On en déduit que $1001 = (45 + 32)(45 - 32) = 77 \times 13$. Nous expliquons tout cela plus précisément dans l'*annexe 2* à la fin de ce document (*page 32*)

4. La méthode de pulvérisation (*kuttaka*)

Il s'agit d'un processus qui consiste à découper les quantités à calculer en morceaux de plus en plus petits, qui deviennent calculables, puis de calculer les quantités initiales en les reconstituant. Ce procédé à été initié par Aryabhata I (années 500) et Baskhara I (600-680), pionniers de ce qui est la période dite classique des mathématiques indiennes, Bhaskhara écrivant des commentaires sur l'oeuvre d'Aryabhata 1, appelée *Aryabhatiya*.

Cette méthode est appliquée pour résoudre en entiers des équations de la forme $a\,x - b\,y = c$, avec a, b, c entiers positifs, et a/b fraction irréductible.

Prenons un exemple, avec $a = 27$, $b = 62$ et $c = 2$, soit $27\,x - 62\,y = 2$. Dans la colonne des « restes », on place 62 (le plus grand des deux nombres) suivi de 27. Puiq on fait 62 / 27, ce qui donne comme quotient 2 et comme reste 8. Le quotient 2 est placé dans la colonne (la « liane ») des quotients, et le reste 8 sous le 27 de la colonne des restes. Puis on recommence en faisant 27 / 8, etc. jusqu'à avoir un reste égal à 1. On met toujours c et 0 pour les deux derniers éléments de la colonne des restes.

restes	quotients avec en plus à la fin $c = 2$ suivi de 0
62	2
27	3
8	2
3	1
2	2
1	0

On vient d'obtenir la « liane » de la « pulvérisation ».

Puis on fait la remontée à partir du bas de la « liane », en appliquant la règle sur les 3 éléments successifs m, n, p :

$m \rightarrow mn + p$
$n \rightarrow n$
p

La liane se raccourcit d'un cran à chaque étape, jusqu'à la fin où il reste deux nombres, qui sont x et y (ou y et x).

2	2	2	2	46
3	3	3	20	20
2	2	6	6	
1	2	2		
2	2			
0				

On a trouvé $x = 46$, $y = 20$, et l'on a bien $27 \times 46 - 62 \times 20 = 2$. Ici (46, 20) est la plus petite solution positive. Il existe une infinité de solutions positives $x = 46 + k \times 62$, $y = 20 + k \times 27$ ($k \geq 0$).

Autre exemple : $27\,x - 44\,y = 3$

44	1	1	1	1	1	39	$x = 39$ et $y = 24$, mais $27 \times 39 - 44 \times 24 = -3$.
27	1	1	1	1	24	24	
17	1	1	1	15	15		
10	1	1	9	9			
7	2	6	6				
3	3	3					
1	0						

En fait, la méthode résout $ax - b\,y = c$ ou $a\,x - by = -c$ selon la parité de la taille des colonnes.

Remarques :

- Si l'on veut résoudre $27x - 62y = 6$, on trouve $x = 138$, $y = 60$. Ce n'est pas la plus petite solution positive, celle-ci étant $x = 138 - 2\times 62 = 14$, $y = 60 - 2\times 27 = 6$.

- Si l'on veut résoudre $62x - 27y = 6$, on trouve aussi $x = 60$, $y = 138$, mais alors $62\times 60 - 138\times 27 = -6$. Il convient de prendre $x = -60$, $y = -138$, puis $x = -60 + 3\times 27 = 21$ et $y = -138 + 3\times 62 = 48$.

- Le cas le plus simple est celui où $c = 1$. On est alors sûr d'obtenir la plus petite solution positive (ou négative) ici de $27x - 62y = 1$, soit $x = 23$ et $y = 10$. Mais pour $62x - 27y = 1$, il convient de prendre $x = -10$ et $y = -23$, puis $x = -10 + 27 = 17$, et $y = -23 + 62 = 39$.

- En fait, la liane de la pulvérisation, sauf ses deux derniers éléments, n'est autre que l'écriture de 62/27 sous forme de fractions continuées, jusqu'à l'avant-dernière réduite, qui est 23 /10, avec $x = 23$ et $y = 10$, solution de $27x - 62y = 1$:

$$\frac{62}{27} = 2 + \frac{1}{\frac{27}{8}} = 2 + \frac{1}{3 + \frac{1}{\frac{8}{3}}} = 2 + \frac{1}{3 + \frac{1}{2 + \frac{1}{\frac{3}{2}}}} = \mathbf{2} + \frac{1}{\mathbf{3} + \frac{1}{\mathbf{2} + \frac{1}{\mathbf{1} + \frac{1}{2}}}}$$

Mais au lieu de calculer les réduites successives en descente, la méthode indienne pratique une remontée.

Cette méthode est surtout utilisée pour trouver un nombre N dont on connaît le reste lorsqu'on le divise par un nombre donné, et aussi le reste lorsqu'on le divise par un deuxième nombre.

Par exemple, trouver N tel que, divisé par 27, cela donne un reste 3, et divisé par 62, le reste soit 5, ce qui signifie :

$N = 27x + 3$ et $N = 62y + 5$, d'où $27x - 62y = 2$. On a trouvé comme solution $x = 46$, $y = 20$. D'où $N = 1245$.

Cela correspond si l'on veut à :
$N = 3$ [27]
$N = 5$ [62]
On est alors dans les conditions du théorème chinois, qui donne aussi $N = 1245$ [1674].

Ce type de problème devient même populaire, jusque dans les basses castes de la société indienne. Comme par exemple cette devinette mathématique connue dans des villages pauvres de la région du Tamil Nadu (le pays tamoul en Inde du Sud) :

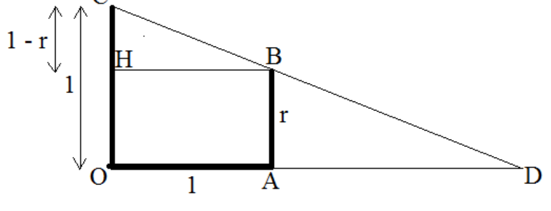
Un marchand d'oeufs itinérant se bat avec un vagabond le long d'un chemin. Dans la bagarre tous ses oeufs sont brisés. Devant le conseil du village, le marchand demande réparation. Les membres du conseil lui demandent combien d'oeufs ont été cassés. Il répond :
« Si je les comptais deux par deux, il en resterait un. Si je les comptais trois par trois, il en resterait deux. Si je les comptais quatre par quatre, il en resterait trois. Si je les comptais cinq par cinq, il en resterait quatre. Si je les comptais sept par sept, il n'en resterait pas. »[8]

5. Arithmétique de l'infini

Au 14è siècle, Madhava crée l'Ecole de Mathématiques et d'Astronomie du Kerala. Au 15è siècle, Nilakantha est son principal successeur. L'Ecole est florissante pendant plus de deux siècles. Tout en reprenant les travaux de leurs prédécesseurs, les mathématiciens de l'école du Kerala ont comme originalité de s'être intéressés aux sommations infinies, en commençant par la série géométrique.

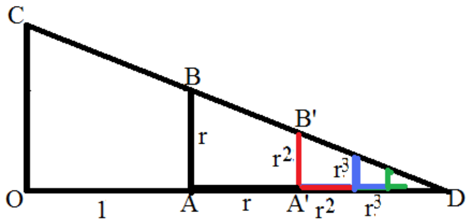
5.1. Série géométrique

La formule devenue classique $1 + r + r^2 + r^3 + ... = \frac{1}{1-r}$ pour $0 < r < 1$ est démontrée géométriquement grâce au dessin suivant :



On construit le trapèze rectangle $OABC$ avec une base de longueur 1, et des côtés latéraux de longueur 1 et r. On en déduit le triangle ODC. Les triangles HBC et ODC étant homothétiques, on en déduit que $OD / HB = OC / HC$, soit
$OD = 1 / (1 - r)$.

[8] Le nombre cherché N est impair. Il doit aussi vérifier $N = 2$ [3], $N = 3$ [4], $N = 4$ [5] , $N = 0$ [7]. L'application du théorème chinois donne $N = 119$ [420] qui est aussi un nombre impair. On trouve comme solutions 119, puis 539, etc. Dans le contexte du village concerné, la solution acceptable est 119.



Maintenant plaçons A' sur $[OD]$ tel que $AA' = AB = r$, puis traçons le segment vertical $[A'B']$ et vérifions que $A'B' = r^2$. L'homothétie de centre D et de rapport r transforme le triangle DOC en DAB. De plus $[OA]$ de longueur 1 devient $[AA']$ de longueur r. La même homothétie transforme le triangle DAB en $DA'B'$, d'où $A'B' / AB = r$, et $A'B' = r^2$. Puis on répète la même construction avec $A'A'' = r^2$, ce qui entraîne $A''B'' = r^3$ (en bleu sur le dessin), etc. Finalement, en passant à la limite :

$OA + AA' + A'A'' + ... = 1 + r + r^2 + r^3 + ... = OD = 1 / (1 - r)$.

D'autre part, avec un nombre fini de termes, on a la formule : $1 + r + r^2 + ... + r^n = (1 - r^{n+1}) / (1 - r)$. Les mathématiciens du Kerala présentent le calcul de cette formule de la façon suivante :

$S = 1 + r + r^2 + ... + r^n$
$(1 - r)\, S = 1 - r + r\,(1 - r) + r^2(1 - r) + ... + r^n\,(1 - r) = 1 - r^{n+1}$ après simplifications.

5.2. Approximation de sommes

Connaissant les formules sur les sommes de nombres successifs, de leurs carrés et de leurs cubes, les mathématiciens indiens en déduisent que pour n grand :

$$1+2+3+...+n \approx \frac{n^2}{2}$$

$$1^2+2^2+3^2+...+n^2 \approx \frac{n^3}{3}$$

$$1^3+2^3+3^3+...+n^3 \approx \frac{n^4}{4}$$

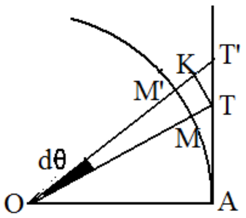
Et ils généralisent[9] :

$$1^p+2^p+3^p+...+n^p \approx \frac{n^{p+1}}{p+1}$$

5.3. Approximation du nombre pi

En Europe, on doit à Wallis (1655), Gregory (1672), Leibniz (1674) des formules d'approximation du nombre π, notamment :

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



Pour établir cette formule, leur idée consiste à découper l'angle de 45° en n petits angles égaux $d\theta$ dans le cercle de rayon unité, avec l'arc MM' égal à $d\theta$, $TT' = d(\tan\theta)$ et $AT = \tan\theta$ (voir dessin). En projetant T sur (OT') en K, les triangles TKT' et OAT sont smblables, $TT' / TK = OT / OA$, d'où :

$TT' = TK \times OT$.

Les triangles OMM' et OTK sont homothétiques, $TK / MM' = OT / OM$, et en assimilant la corde MM' à l'arc, $TK = OT\, d\theta$. Finalement :

$TT' = OT^2\, d\theta = (1 + AT^2)\, d\theta$, $d(\tan\theta) = (1 + \tan^2\theta)\, d\theta$.

$$d\theta = \frac{d(\tan\theta)}{1+\tan^2\theta} = \frac{dt}{1+t^2}$$ en posant $t = \tan\theta$.

Par sommation de ces $d\theta$ entre 0 et $\pi/4$, on obtient $\pi/4$, et cela revient à sommer les dt entre 0 et 1 :

$$\frac{\pi}{4} = \int_0^1 \frac{dt}{1+t^2} = \int_0^1 (1-t^2+t^4-t^6+...)dt = [t-\frac{t^3}{3}+\frac{t^5}{5}-...]_0^1 = 1-\frac{1}{3}+\frac{1}{5}-...$$

---

[9] Ces formules de sommation avaient aussi été trouvées par Ibn Al-Haytham, aussi appelé Alhazen (965- 1039) qui vécut à Bagdad, à Bassorah, puis au Caire. Ses calculs sur les sommes de puissance l'ont même amené à trouver la formule pour les puissances quatrièmes.

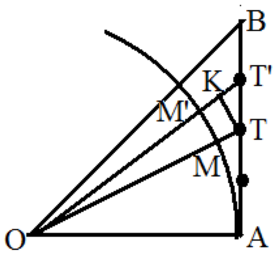
$$\sum_{k=1}^{n} k^4 = \frac{n^5}{5}+\frac{n^4}{2}+\frac{n^3}{3}-\frac{n}{30}$$

Il est possible que ses travaux dans ce domaine aient inspirés les savants indiens.

On a trouvé la formule cherchée, celle-ci étant un cas particulier de l'expansion de la fonction *atan* :
$a\tan t = 1 - \frac{t^3}{3} + \frac{t^5}{5} - \frac{t^7}{7} + ...$ ou $\theta = \tan\theta - \frac{\tan^3\theta}{3} + \frac{\tan^5\theta}{5} - \frac{\tan^7\theta}{7} + ...$

Un ou deux siècles auparavant, Madhava et Nilakantha trouvent aussi cette formule, en s'y prenant autrement. Au lieu de découper l'angle en petits angles égaux, ils découpent le segment où se trouvent les tangentes en segments de même longueur, ce qui aboutit à une méthode complètement différente.

La méthode de Madhava-Nilakantha



Prenons l'angle $\pi/4$ dans le cercle trigonométrique, avec $AB = 1$. Découpons $[AB]$ en n segments de même longueur. Prenons un morceau $TT' = 1/n$. Les triangles OAT et TKT' sont semblables :

$TK / TT' = 1 / OT$, $TK = 1 / (n\, OT)$.

Les triangles OMM' et OTK sont homothétiques :
$MM' / TK = 1 / OT$, $MM' = TK / OT$.

Finalement $MM' = \frac{1}{n\, OT^2} = \frac{1}{n}\frac{1}{1+(\frac{k}{n})^2}$, et

$\frac{\pi}{4} = \frac{1}{n}\sum_{k=0}^{n-1}\frac{1}{1+(\frac{k}{n})^2} = \frac{1}{n}\sum_{k=0}^{n-1}(1-(\frac{k}{n})^2+(\frac{k}{n})^4-(\frac{k}{n})^6+...)$ avec une double sommation

$= (1/n)\,(1)$
$+ (1/n)\,(1-(1/n)^2+(1/n)^4-(1/n)^6+...)$
$+ (1/n)\,(1-(2/n)^2+(2/n)^4-(2/n)^6+...)$
...
$+ (1/n)\,(1-((n-1)/n)^2+((n-1)/n)^4-((n-1)/n)^6+...)$

$= 1-(1/n^3)\,(1^2+2^2+...+(n-1)^2)+(1/n^5)\,(1^4+2^4+...+(n-1)^4)-(1/n^7)\,(1^6+2^6+...+(n-1)^6)+...$
où l'on a fait une sommation en colonnes
$= 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+...$ cela grâce à la formule $\frac{1}{n^{p+1}}(1^p+2^p+3^p+...+(n-1)^p \approx \frac{1}{p+1}$

En s'apercevant que la sommation de $1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+...$ vers $\frac{\pi}{4}$ est très lente, Madhava et Nilakantha vont ajouter des termes correcteurs pour accélérer la convergence.

Ajout de termes correcteurs

Prenons la formule jusqu'à un rang $n-1$ et ajoutons un terme correctif $(-1)^n F(n)$, pour s'approcher plus vite de $\pi/4$:
$$\frac{\pi}{4} \approx 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+...+\frac{(-1)^{n-1}}{2n-1}+(-1)^n F(n)$$

Mais comment choisir $F(n)$?

Ecrivons la formule jusqu'au rang n :
$$\frac{\pi}{4} \approx 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+...+\frac{(-1)^{n-1}}{2n-1}+\frac{(-1)^n}{2n+1}+(-1)^{n+1}F(n+1)$$

On veut que la différence entre les développements au rang $n-1$ et au rang n soit la plus proche de 0 possible. Or cette différence est :
$$(-1)^{n+1}(F(n+1)+F(n)-\frac{1}{2n+1})$$
ce qui invite à choisir $F(n) = \frac{1}{4n}$.

On a alors : $F(n+1)+F(n)-\frac{1}{2n+1} = \frac{1}{4(n+1)}+\frac{1}{4n}-\frac{1}{2n+1} = \frac{1}{4n(n+1)(2n+1)} \approx \frac{1}{8n^3}$

L'erreur est de l'ordre de $1/n^3$.

Madhava et Nilakantha sont même allés plus loin, en prenant :

$F(n)=\dfrac{1}{4n+\dfrac{1}{n}}=\dfrac{n}{4n^2+1}$. On constate alors par le calcul que l'erreur est de l'ordre de $\dfrac{1}{8n^5}$.

Ils ont fait mieux encore, avec

$F(n)=\dfrac{1+\dfrac{1}{n^2}}{4n+\dfrac{5}{n}}=\dfrac{n^2+1}{4n^3+5n}$.

En utilisant seulement $n = 21$ termes, ils trouve π avec 13 décimales exactes.[10]

Sans terme correcteur, Nikalantha choisit aussi $\theta = \pi/3$ au lieu de $\pi/4$ dans la formule initialement trouvée, ce qui donne $\pi=\sqrt{12}(1-\dfrac{1}{3\times 3}+\dfrac{1}{3^2\times 5}-\dfrac{1}{3^3\times 7}+...)$, où il suffit de 21 termes pour avoir π avec 11 décimales.

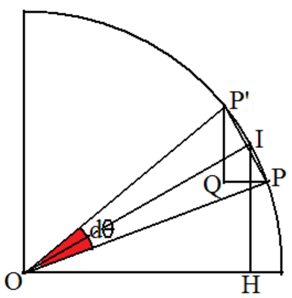
On attribue aussi à Nilakantha d'autres formules, comme :

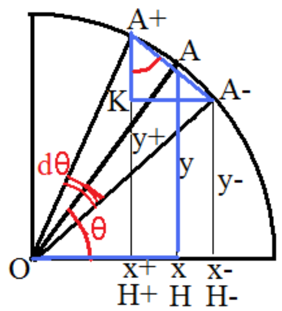
$$\frac{\pi}{4}=\frac{3}{4}+\frac{1}{2\times 3\times 4}-\frac{1}{4\times 5\times 6}+\frac{1}{6\times 7\times 8}-\frac{1}{8\times 9\times 10}$$

$$\pi=3+\sum_{n\geq 1}\frac{(-1)^{n+1}}{n(n+1)(2n+1)}$$

5.4. Premières dérivations de fonctions trigonométriques

Là encore, Madhava et Nilakantha utilisent une méthode géométrique. Voici comment ils s'y prennent pour trouver ce que l'on appelle de nos jours les dérivées du sinus et du cosinus.





Dans le cercle de rayon unité, l'arc PP' correspond à un petit angle $d\theta$. A partir de I milieu de la corde PP' assimilée à l'arc, on construit le triangle rectangle OHI, ainsi que le triangle rectangle $PP'Q$ (voir dessin). Ces deux triangles ont leurs côtés respectifs perpendiculaires. Ils sont semblables, et $QP' / OH = PP' / OP$, d'où $QP' = OH \times PP'$. Or $OH = \cos\theta$ et $QP' = d(\sin\theta)$.

Finalement $d(\sin\theta) = \cos\theta\, d\theta$.

De même, $d(\cos\theta) = - QP = - HI \times PP'$, et $d(\cos\theta) = - \sin\theta\, d\theta$.

Par un procédé de doubles sommations, comme précédemment, Madhava et Nilakantha trouvent aussi le développement en série du sinus et du cosinus :

$\sin\theta = \theta - \theta^3/6 + \theta^5/120 - ...$ et $\cos\theta = 1 - \theta^2/2 + \theta^4/24 - ...$

Voici des indications sur leur démonstration. [11]

Commençons par prendre un angle θ et une petite variation $d\theta$ de part et d'autre de θ avec $A\text{-}\,A = AA+ = d\theta/2$. Les triangles OHA et $A+KA\text{-}$ étant semblables, on en déduit que :

$A\text{-}\,K / A\text{-}\,A+ = HA / OA$, soit avec $OA = 1$:

$(x\text{-} \; - x+) / d\theta = y$ ou encore

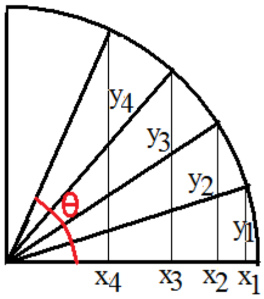
$\cos(\theta + d\theta/2) - \cos(\theta - d\theta/2) = - \sin\theta\, d\theta$.

On a aussi $A+\,K / A\text{-}\,A+ = OH$, soit $(y+ - y\text{-}) / d\theta = y$ ou encore

$\sin(\theta + d\theta/2) - \sin(\theta - d\theta/2) = \cos\theta\, d\theta$.

[10] Le calcul approché de π fait l'objet de recherches intenses dans toutes les civilisations anciennes Notamment, Archimède (-3è siècle) utilise un polygone à 96 côtés pour obtenir l'encadrement $223/71 < \pi < 22/7$ avec 3 décimales assurées derrière la virgule. En Chine, Zu Chongzhi (5è siècle) prend $\pi = 22/7$ et $355/113$ avec 7 décimales assurées (355/113 est la 4è réduite de π). En Inde, dès le 6è siècle, Aryabhatiya obtient π avec 4 décimales. Dans le monde musulman, en 1424, Al Kashi arrive à 17 décimales.

[11] Cette démonstration est reprise du document [KAT1995]



Maintenant découpons l'angle θ en n petits angles égaux $d\theta = \theta / n$ (pour bien voir, on a pris $n = 4$ sur le dessin).

$x_n - x_1 = (x_n - x_{n-1}) + (x_{n-1} - x_{n-2}) + ... + (x_2 - x_1)$

$= -(\theta / n)(y_{n-1} + y_{n-2} + y_{n-3} + ... + y_1)$ d'après les formules précédentes en assimilant y_i associé à l'angle $\theta_i = i\, d\theta$ et le y associé à l'angle $\theta_i + d\theta/2$.

Lorsqu'à son tour l'angle θ est petit, on a $x_1 \approx 1$ et $y_i \approx i\theta / n$ en assimilant la corde et l'arc. Avec $x_n = \cos\theta$, cela donne :

$$\cos\theta \approx 1 - (\theta^2 / n^2)(1 + 2 + 3 + ... + (n-1))$$
$$\approx 1 - (\theta^2 / n^2) n(n-1)/2$$
$$\approx 1 - \theta^2 / 2$$

Recommençons avec le sinus :

$y_n = (y_n - y_{n-1}) + (y_{n-1} - y_{n-2}) + ... + (y_2 - y_1) + y_1$

avec $\Delta y_n = y_n - y_{n-1} = (\theta / n)\, x_n$

$\Delta y_{n-1} = y_{n-1} - y_{n-2} = (\theta / n)\, x_{n-1}$

...

$\Delta y_2 = y_2 - y_1 = (\theta / n)\, x_2$

$\Delta y_1 = y_1 = (\theta / n)\, x_1$

Passons aux difféences secondes :

$\Delta y_2 - \Delta y_1 = (\theta / n)(x_2 - x_1) = -(\theta / n)^2 y_1$ ou $\Delta y_2 - y_1 = -(\theta / n)^2 y_1$

$\Delta y_2 = y_1 - (\theta / n)^2 y_1$

$\Delta y_3 - \Delta y_2 = (\theta / n)(x_3 - x_2) = -(\theta / n)^2 y_2$ ou $\Delta y_3 = \Delta y_2 - (\theta / n)^2 y_2$

$\Delta y_3 = y_1 - (\theta / n)^2 y_1 - (\theta / n)^2 y_2 = y_1 - (\theta / n)^2 (y_1 + y_2)$

$\Delta y_4 - \Delta y_3 = (\theta / n)(x_4 - x_3) = -(\theta / n)^2 y_3$ ou $\Delta y_4 = \Delta y_3 - (\theta / n)^2 y_3$

$\Delta y_4 = y_1 - (\theta / n)^2 (y_1 + y_2) - (\theta / n)^2 y_3 = y_1 - (\theta / n)^2 (y_1 + y_2 + y_3)$

et ainsi de suite par substitutions progressives. Finalement :

$\sin\theta = y_n = \Delta y_1 + \Delta y_2 + ... + \Delta y_n$

$= n\, y_1 - (\theta / n)^2 (y_1 + (y_1 + y_2) + (y_1 + y_2 + y_3) + (y_1 + y_2 + ... + y_{n-1}))$

Lorsque θ est petit, avec $y_i \approx i\theta / n$

$\sin\theta = \theta - (\theta / n)^2 (\theta / n + (\theta / n + 2\theta / n) + ... + (\theta / n + 2\theta / n + 3\theta / n + ... + (n-1)\theta / n)$

$= \theta - (\theta / n)^3 (1 + (1 + 2) + (1 + 2 + 3) + ... + (1 + 2 + 3 + ... + (n-1))$

On retrouve la somme des nombres triangulaires :

$\sin\theta = \theta - (\theta / n)^3\, n\,(n + 1)(n + 2) / 6$

$\sin\theta \approx \theta - \theta^3 / 6$

Les mathématiciens indiens n'en sont pas restés là. Après l'approximation $y_i \approx i\theta / n$, les calculs sont repris avec $y_i \approx i\theta / n - (i\theta / n)^3 / 6$, ce qui va donner :

$\cos\theta \approx 1 - \theta^2 / 2 + \theta^4 / 24$ puis $\sin\theta \approx \theta - \theta^3 / 6 + \theta^5 / 120$

Et l'on pourrait encore continuer, ce qui donne le développement en série de puissances du sinus et du cosinus.

Par leur ingéniosité stupéfiante, Madhava et Nilakantha, ainsi que d'autres membres de l'Ecole de matéhmatiques et d'astronomie du Kerala, apparaissent comme des précurseurs du calcul infinitésimal, bien avant leurs homologues européens comme Leibniz, Barrow, Newton ... au I7è siècle.

Y a-t-il eu pour autant transmission des connaissances de l'Inde vers l'Europe ? Il n'existe aucune preuve absolue dans un sens ou dans l' autre. Ce qui va en faveur de la transmission, c'est la grande activité commerciale qui se développe à cette époque entre la côte de Malabar et l'Europe, ainsi que la présence importante de missionnaires jésuites au Kerala. Des documents venant d'Inde se retrouvent en Italie, et les visites de Gregory et de Mersenne dans ce pays peuvent avoir joué un rôle. On peut même imaginer que Gregory s'en est inspiré pour sa formule, et que Fermat n'a pas trouvé tout seul le cas d = 61 dans ce qui deviendra l'équation de Pell. Il s'agit là d'une éventualité que certains historiens indiens estiment plausible.[12]

---

[12] Ils font remarquer que de leur côté des experts européens ne se sont pas génés pour faire état de transmissions de l'ouest vers l'est, sans voir que cela ait pu se passer en sens inverse. G.H. Joseph cite B. L. Van der Waerden qui, dans les années 1980, proclame que la trigonométrie d'Ayabhata a été empruntée aux Grecs, et que le travail de Bhaskara II sur les équations diophantiennes provient d'un manuscrit grec inconnu (dans un article *Pell'equation in the mathematics of the Greeks and Indians*, paru à l'origine en russe dans la revue *Uspekhi Mat. Nauk.* 31., 1976, puis traduit en anglais). Mais Van der Waerden conclut que « dans l'histoire des sciences les inventions

D'autres arguments vont en défaveur de cette transmission. D'abord les ouvrages des mathématiciens de l'Ecole du Kerala sont écrits dans une langue locale (*le malayalam*), ce qui a fortement ralenti la diffusion de leurs idées. Mais surtout les méthodes indiennes de calcul infinitésimal sont nettement différentes de celles qui vont être mises en oeuvre par les européens. A force de jongler avec des sommations de sommations de sommations, les savants indiens ne semblent pas avoir vu le lien entre la tangente à une courbe et la dérivée, ni celui entre les aires et le calcul intégral, pourtant déjà entrevu par Archimède. Notamment ils n'ont pas fait le lien entre leur fameuse formule

$\frac{1^p + 2^p + 3^p + ... + n^p}{n^{p+1}} \approx \frac{1}{p+1}$ et l'aire située sous une courbe d'allure parabolique (ou encore l'intégrale de la fonction x^p).[13]

Cela peut expliquer une certaine stagnation des mathématiques indiennes après cette période florissante qui va jusqu'au début du 17è siècle. Pour couronner le tout, de 1750 à 1947, la colonisation britannique ne va pas arranger les choses.

6. Equation de Pell $x^2 - d\,y^2 = 1$

L'intérêt pour ce genre d'équation en Europe commence en 1667 lorsque Fermat défie ses collègues mathématiciens au sujet de cette équation notamment pour $d = 61$ et $d = 109$.[14]

« *J'attends la solution de ces questions. Si elle n'est fournie ni par l'Angleterre ni par la Gaule Belgique ou Celtique, elle le sera par la Gaule de Narbonne.* »

Plusieurs mathématiciens participent à ce *challenge*, notamment Frénicle de Bessy (la Gaule Celtique), Brouncker et Wallis (les Anglais)[15]. Ces trois confrères de Fermat trouvent des méthodes de résolution, des démonstrations partielles, et apportent de nombreux résultats.

Brouncker va jusqu'à donner la réponse pour un cas très complexe, $d = 313$, en précisant qu'il lui a fallu « une heure ou deux » pour y arriver, peut-être pour se moquer de Fermat qui n'a rien fait :

$x = 32\,188\,120\,829\,134\,849$, $y = 1\,819\,380\,158\,564\,160$

Il faudra attendre les travaux d'Euler (1707-1783) puis de Lagrange (1736-1813) pour avoir les démonstrations complètes, via l'utilisation des fractions continuées. Mais au 7è siècle, 1000 ans avant Fermat, Brahmagupta avait posé les jalons essentiels d'une méthode de résolution, suivi au 12è sicèle par Bhaskara II qui donne une méthode légèrement différente de l'approche aujourd'hui classique par les fractions continuées, et qui reste de nos jours un peu plus performante.

Bhaskara II et peut-être aussi Brahmagupta traitent notamment l'exemple $d = 61$ posé par Fermat, surtout pour montrer l'efficacité de leur méthode expérimentale dans un cas qu'on aurait pu croire complexe, alors que Fermat voit plutôt la complexité du problème.

---

indépendantes sont exceptionnelles : la règle générale est la dépendance. » Cela devrait inviter à plus de modestie quelques intellectuels indiens actuels affirmant que l'Inde est le « berceau des mathématiques », voire « de l'humanité ». Il n'y a pas de berceau !

[13] Si les mathématiciens indiens ont été des pionniers en matière de calcul infinitésimal, ils ont été suivis par une armada de mathématiciens et physiciens en Europe au 17è siècle. Ceux-ci ont littéralement explosé le calcul infinitésimal. Il y eut d'abord Cavalieri, un jésuite italien (tiens-tiens !) en 1620, et le fançais Roberval, celui de la balance. Puis Torricelli, Angeli (un autre jésuite italien), Fermat et Descartes, Wallis, Barrow, Huygens, Leibniz et Newton. Dans cette liste, on notera le mélange entre mathématiques et physique, et notamment la mécanique. Ce lien entre physique et mathématiques semble avoir manqué aux mathématiciens indiens.

[14] Précisons que le nombre d est un entier positif qui ne doit pas être un carré parfait. Les solutions (x, y) doivent être des nombres entiers positifs.

Bien avant notre ère, ce type d'équation transparaît en Inde, avec l'exemple $2 \times 408^2 + 1 = 577^2$ ou chez Archimède qui écrit $1351 / 780 > \sqrt{3}$ (ce qui correspond à $3 \times 780^2 + 1 = 1351^2$). Plus tard vers les années 200, Diophante traite aussi ce genre d'équation, mais en s'intéressant aux solutions rationnelles. On doit à Fermat d'avoir relancé le même problème, mais en entiers. Précisons que le nombre d ne doit pas être un carré parfait dans le traitement de l'équation.

[15] Ce défi est mal pris par Wallis qui écrit à un collègue anglais lui aussi défié par Fermat : « Votre très noble correspondant a pris plaisir à provoquer en champ clos non pas un ou deux mathématiciens du commun, mais et l'Angleterre toute entière, et la Belgique et le reste de la Gaule sauf la Narbonnaise... »

Autre anecdote : lorsque Fermat diffuse son problème, les mathématiciens anglais en reçoivent d'abord une version tronquée, après passage par le biais d'intermédiaires. Ils croient que Fermat leur demande une solution utilisant des nombres rationnels, et trouvent ce problème sans intérêt, puisqu'il a une réponse bien connue. En effet, pour $d\,x^2 + 1 = y^2$, il suffit de poser $y = 1 + p/q$, ce qui donne $x = 2\,p\,q / (d\,q^2 - p^2)$ et $y = (d\,q^2 + p^2) / (d\,q^2 - p^2)$.

6.1. La méthode de composition (*samasa bhavana*) de Brahmagupta

Prenons l'équation $x^2 - dy^2 = n$, et si elle admet une solution (a, b), notons $(a, b ; n)$ le triplet correspondant, tel que $a^2 - db^2 = n$. Brahmagupta a découvert comment composer (*samasa bhavana*) deux de ses triplets :

Si l'on a $(a, b ; n)$ et $(a', b'; n')$ alors on a aussi $(aa' + bb'd, ab'+ ba'; nn')$

Cela signifie que si l'on a une solution (a, b) de l'équation $x^2 - dy^2 = n$ et une solution (a', b') de l'équation $x^2 - dy^2 = n'$, alors $(aa' + bb'd, ab'+ ba')$ est une solution de l'équation $x^2 - dy^2 = nn'$.

Pour le vérifier, il suffit de faire le calcul.[16]

Cela va nous aider pour traiter l'équation la plus importante : $x^2 - dy^2 = 1$, et trouver d'autres solutions que la solution évidente (1, 0) sans intérêt. Prenons un exemple simple :

$\mathbf{x^2 - 3y^2 = 1}$

On trouve aussitôt une solution $(a, b) = (2, 1)$.
En composant (2, 1 ; 1) avec lui-même, comme l'a fait Brahmagupta, on trouve (7, 4 ; 1), d'où la solution (7, 4) avec $7^2 - 3\times 4^2 = 1$. Puis on compose ce résultat avec (2, 1 ; 1), et l'on obtient (26, 15; 1), d'où la solution (26, 15). On peut continuer ainsi indéfiniment.[17] C'est ainsi que Brahmagupta trouva que l'équation admettait une infinité de solutions, à partir de l'une d'elles. On en sait un peu plus aujourd'hui : il y a toujours une plus petite solution positive, comme (2, 1) dans notre exemple, et en prenant les puissances α^n, on les obtient toutes. Il n'y en a pas d'autres.

Signalons que les Indiens de cette époque faisaient leurs calculs de tête ou en traçant des diagrammes sur des tablettes couvertes de poussière de craie ou de sable. Voici comment Brahmagupta ou plus tard Baskhara II posaient le problème et présentaient les calculs :

Quel est le nombre dont le produit de son carré par 11, ajouté à 1, est lui-même un carré ?

Il s'agit de $11x^2 + 1 = y^2$, [18] qui n'a pas de solution évidente. Ils choisissent $x = 1$, mais 11 + 1 = 12 n'étant pas un carré, ils prennent y dont le carré est le plus proche de 12, soit $y = 3$. L' «augmentation » $y^2 - 11x^2$ est alors de -2, avec le triplet ($x = 1$, $y = 3$, -2). Puis ils composent ce triplet avec lui-même, ce qu'ils écrivent ainsi :

petit	*grand*	*augmentation*
1	3	-2
1	3	-2

Le produit en croix donne $x = 6$, et le produit de la première colonne, multipliée par 11, ajouté au produit de la deuxième colonne donne $y = 20$. L'augmentation est de $-2\times -2 = 4$, et l'on a :

$11\times 6^2 + 4 = 20^2$. En divisant par 4, on trouve $11\times 3^2 + 1 = 10^2$, d'où la solution $x = 3$, $y = 10$. Et l'on pourrait trouver une deuxième solution en composant (3, 10) avec (3,10) :

3 10 1
3 10 1 d'où $x = 199$ et $y = 60$.

---

[16] On peut le vérifier en utilisant une terminologie plus moderne. Considérons l'anneau des nombres de la forme $\alpha = a + b\sqrt{d}$ avec a et b entiers, où d est un nombre positif qui n'est pas un carré parfait. Le conjugué de α est $\bar{\alpha} = a - b\sqrt{d}$, et l'on dispose des règles de conjugaison classiques : $\overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta}$ $\overline{\alpha\beta} = \bar{\alpha}\ \bar{\beta}$ $\bar{\bar{\alpha}} = \alpha$
On appelle norme de α, ou encore de (a, b) le nombre entier positif ou négatif :
$N(\alpha)$ ou $N(a,b) = \alpha\bar{\alpha} = a^2 - db^2$.
Dans ce contexte le triplet de Brahmagupta n'est autre que $(a, b ; N(a, b))$. On obtient alors la formule :
$N(\alpha\beta) = N(\alpha)N(\beta)$ avec $\alpha = a + b\sqrt{d}$ et $\beta = a' + b'\sqrt{d}$
En effet $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta)$.
Or $\alpha\beta = (a + b\sqrt{d})(a' + b'\sqrt{d}) = aa' + bb'd + (ab' + ba')\sqrt{d}$
Avec $N(\alpha) = n$ et $N(\beta) = n'$, on retrouve bien la formule de Brahmagupta, soit $(aa' + bb'd, ab'+ ba'; nn')$ ou encore $(aa' + bb'd)^2 - d(ab'+ ba')^2 = nn'$.

[17] En appelant (a_1, b_1) le premier couple solution, on obtient ensuite le couple (a_2, b_2), puis (a_3, b_3), etc. On constate grâce aux formules que $a_1 < a_2 < a_3 < \ldots$, et aussi $b_1 < b_2 < b_3 < \ldots$. Les solutions sont donc toutes différentes, il y en a bien une infinité. Autrement dit, en posant $\alpha = a + b\sqrt{d}$, avec $N(\alpha) = 1$, on a aussi $N(\alpha^n) = 1$, ce qui donne une infinité de solutions, car si l'on avait $\alpha^k = \alpha^{k'}$, soit $\alpha^{k-k'} = 1$, cela imposerait que $k - k' = 0$ et $k = k'$ puisque l'on ne prend pas $\alpha = 1$..

[18] Dans cette éccriture, il y a interversion de x et y par rapport à l'équation $x^2 - dy^2 = 1$.

Quitte à procéder par tâtonnements, Brahmagupta a aussi résolu l'équation

$\mathbf{x^2 - 92y^2 = 1}$

Aucune solution simple n'apparaissant, on choisit $y = 1$ et x^2 le plus proche possible de 92, soit $x = 10$. On obtient alors le triplet (10, 1 ; 8) avec $10^2 - 92\times 1^2 = 8$. Puis composons ce triplet avec lui-même, ce qui donne (192, 20, 64), soit $192^2 - 92\times 20^2 = 64$. Divisons tout par 64, quitte à obtenir une fraction :

$24^2 - 92\times(5/2)^2 = 1$, ce qui donne le triplet (24, 5/2; 1).

Enfin composons ce triplet avec lui-même, la fraction va disparaître (car 92 est divisible par 4), et l'on trouve le triplet (1151, 120; 1), d'où la solution (1151, 120).

A partir de ces exemples, Brahmagupta est allé plus loin. Il a montré que si l'on a une solution de l'équation $x^2 - dy^2 = k$, avec $k = -1$ ou $k = \pm 2$ ou $k = \pm 4$, on peut en déduire une solution pour $x^2 - dy^2 = 1$.

- Cas où l'on connaît une solution (a, b) de $x^2 - dy^2 = -1$. En composant $(a, b ; -1)$ avec lui-même, on trouve le triplet $(a^2 + b^2d, 2ab ; 1)$ et le couple $(a^2 + b^2d, 2ab)$ est une solution de $x^2 - dy^2 = 1$.

Exemple : $\mathbf{x^2 - 5y^2 = 1}$. Comme l'équation $x^2 - 5y^2 = -1$ admet la solution évidente (2, 1), on en déduit la solution (9, 4) pour $x^2 - 5y^2 = 1$.

- Cas où l'on connaît une solution (a, b) de $x^2 - dy^2 = \pm 2$. En composant $(a, b, \pm 2)$ avec lui-même, on obtient $(a^2 + d\,b^2, 2ab ; 4)$, soit $(a^2 + d\,b^2)^2 - (2ab)^2 = 4$. Mais $a^2 + d\,b^2 = a^2 - d\,b^2 + 2\,d\,b^2 = \pm 2 + 2\,d\,b^2$, $a^2 + d\,b^2$ est un multiple de 2. On peut diviser par 4 les deux membres de l'égalité précédente, ce qui donne
$(\frac{a^2+db^2}{2})^2 - d(ab)^2 = 1$, et la solution $(\frac{a^2+db^2}{2}, ab)$ pour $x^2 - dy^2 = 1$. Cette solution correspond à $\alpha^2/2$ pour $\alpha = a + b\sqrt{d}$.

Exemples :

1) $\mathbf{x^2 - 98y^2 = 1}$.
On constate que l'équation $x^2 - 98y^2 = 2$ admet la solution évidente. (10, 1). On en déduit (en prenant $\alpha^2/2$) que ((100+98)/2, 20/2), soit (99, 10) est solution de $x^2 - 98y^2 = 1$.

2) $\mathbf{x^2 - 83y^2 = 1}$.
On constate que l'équation $x^2 - 83y^2 = -2$ admet la solution évidente. (9, 1). On en déduit (en prenant $\alpha^2/2$) que ((81+83)/2, 18/2), soit (82, 9) est solution de $x^2 - 83y^2 = 1$.

- Cas où l'on connaît une solution (a, b) de $x^2 - dy^2 = \pm 4$.

Si a et b étaient pairs, on diviserait par 4 et l'on aurait une solution de $x^2 - dy^2 = 1$. Ce cas est sans intérêt. On verra aussi plus bas, en appliquant la méthode de Bhaskhara II, qu'au cours des calculs a et b sont toujours premiers entre eux : ils ne peuvent pas être pairs tous les deux. On distingue alors deux cas.

- *Premier cas* : a et b n'étant pas tous les deux pairs, supposons que non seulement d n'est pas un carré parfait, mais n'est pas un multiple de 4. Montrons que cela impose que d soit impair.

Si d était pair, avec $a^2 - db^2 = \pm 4$, alors a^2 serait un nombre pair, et a le serait aussi. Dont a^2 serait multiple de 4, $db^2 = a^2 \mp 4$ serait multiple de 4. Comme d n'est pas multiple de 4, 2 doit diviser b^2 et par suite b. Alors a et b seraient pairs tous les deux, ce qui est contraire à notre hypothèse.

Dans ce contexte, b doit être impair. En effet, si b était pair, db^2 serait multiple de 4 et $a^2 = db^2 \pm 4$ serait multiple de 4, a serait pair. Mais a et b ne sont pas tous les deux pairs en même temps. Donc b ne peut être qu'impair.

Maintenant, avec $\alpha = a + b\sqrt{d}$, formons $\alpha^3 = (a + b\sqrt{d})^3 = a^3 + 3dab^2 + (3a^2b + db^3)\sqrt{d}$ et l'on obtient le triplet $(a^3 + 3dab^2, 3a^2b + db^3 ; \pm 64)$, soit
$(a^3 + 3dab^2)^2 - d\,(3a^2b + db^3)^2 = \pm 64$. On constate que :
$a^3 + 3dab^2 = a(a^2 + 3db^2) = a(a^2 - db^2 + 4db^2) = a(\pm 4 + 4db^2) = 4a(\pm 1 + db^2)$.
Avec d et b impairs comme on l'a vu, db^2 est impair, et $db^2 \pm 1$ est pair. Ainsi $a^3 + 3ab^2$ est divisible par 8,
$(a^3 + 3ab^2)/8$ est un entier.

De même, $3a^2b + db^3 = b(3a^2 + db^2) = b(3a^2 - 3db^2 + 4db^2) = b(3\times\pm4 + 4db^2) = 4b(\pm3 + db^2)$ avec ici aussi $\pm3 + db^2$ pair, donc ($3a^2b + db^3$)/8 est un entier.

En divisant l'égalité précédemment trouvée par 64, il reste :

$$(\frac{a^3 + 3dab^2}{8})^2 - d\,(\frac{3a^2b + b^3d}{8})^2 = \pm1$$

Si c'est +1, on a la solution $((a^3 + 3dab^2)/8,\ (3a^2b + b^3d)/8)$ pour $x^2 - dy^2 = 1$.

Si c'est – 1, on compose la solution précédente avec elle-même, ce qui correspond à $\alpha^6/64$, pour avoir $x^2 - dy^2 = 1$.

Exemple : $x^2 - 61y^2 = 1$

Brahmagupta peut-être, ou seulement Bhaskara II plus tard, remarquèrent que l'on avait le triplet (39, 5, –4), soit $39^2 - 61 \times 5^2 = -4$. Avec 39 et 5 tous deux impairs (et 61 non divisible par 4), on a alors, grâce au résultat précédent :

$(a^3 + 3dab^2)/8 = 29718$, et $(3a^2b + b^3d)/8 = 3805$. Il reste à composer (29728, 3805 ; –1) avec lui-même, ce qui donne :

$29728^2 + 61 \times 3805^2 = 1\,766\,319\,049$,
$2 \times 29718 \times 3805 = 226\,153\,980$

C'est le couple solution pour $x^2 - 61y^2 = 1$. On vient de trouver la solution la plus petite, mais formée de grands nombres, en seulement quelques étapes de calcul. C'est un bon exemple de l'efficacité de la méthode, sous réserve que l'on air trouvé par râtonnements le triplet (39, 5, -4).

- *Deuxième cas* : a et b n'étant pas tous deux pairs, d n'est pas un carré parfait mais est un multiple de 4, ce qui impose que a soit pair et b impair, comme on va le vérifier.

En effet, avec $a^2 - db^2 = \pm 4$, et $d = 4d'$, $a^2 = db^2 \pm 4 = a^2 = 4d'b^2 \pm 4$, a^2 est multiple de 4, et a est pair, et par suite b est impair.

Partons du triplet (a, b ; ± 4). En divisant par 4, on obtient le triplet ($a/2$, $b/2$, ± 1), où $a/2$ est entier, mais $b/2$ ne l'est pas. Mais la formule de composition fonctionne encore. Composons le triplet avec lui-même, ce qui donne ($(a^2 + db^2)/4$, $ab/2$; 1). Avec $a/2$ entier et $a^2/4$ entiers, on a aussi $db^2/4$ entier puisque 4 divise d. On a trouvé la solution entière ($(a^2 + db^2)/4$, $ab/2$). C'est justement ce qu'a fait Brahmagupta pour traiter $x^2 - 92y^2 = 1$, comme on l'a vu ci-dessus.

A ce stade, si l'on est capable de trouver une solution de $x^2 - dy^2 = n$ avec $n = \pm 1$ ou ± 2 ou ± 4, on est assuré d'avoir une solution de $x^2 - dy^2 = 1$, et ensuite d'en trouver une infinité.

Mais cela peut demander beaucoup de tâtonnements. Si Brahmagupta a vraiment trouvé la solution (39, 5) vérifiant $x^2 - 61y^2 = -4$, cela lui a ensuite permis de résoudre $x^2 - 61y^2 = 1$. Mais prenons par exemple $x^2 - 13y^2 = 1$. On commence toujours par prendre la valeur la plus simple de y, soit $b = 1$. Puis en choisissant a tel que $|a^2 - d|$ soit le plus petit possible, on trouve $a = 4$, et l'on a le triplet (4, 1 ; 3) qui ne nous est d'aucun secours. Il faudrait de nombreux tâtonnements pour arriver au triplet (18, 5 ; –1) qui nous permettrait de conclure. Pour avoir une méthode générale de résolution, un nouveau procédé était requis, et c'est ce que découvrit le savant indien Bhaskara II vers 1150, avec la méthode *chakravala*.

6.2. La méthode circulaire (*chakravala*) de Bhaskara II

6.2.1. L'algorithme *chakravala*

La méthode circulaire est un algorithme qui permet d'obtenir la plus petite solution de $x^2 - d\,y^2 = 1$. A l'étape 0, on part du triplet (1, 0, 1), solution évidente mais sans intérêt. Puis l'algorithme calcule à chaque étape des triplets (a_j, b_j, k_j) jusqu'à ce que l'on retombe sur une valeur de k égale à 1, ce qui permet d'avoir la première solution non évidente de l'équation. En continuant de même, on aurait un retour périodique de k à 1, avec d'autres solutions de plus en plus grandes de l'équation. D'où la dénomination « cyclique » (ou circulaire) attribuée à cette méthode

En fait, on va avoir besoin à chaque étape de calculer 4 nombres : m_j et le triplet (a_j, b_j, k_j) . A l'étape 0, on prend m_0 tel que m_0^2 soit le plus proche de d possible, et le triplet (1, 0, 1). Mais pour mieux comprendre la méthode de Bhaskara II, nous préférons commencer à l'étape 1.[19]

Prenons m_1 tel que son carré soit le plus proche de d possible, ce qui permet d'obtenir le triplet (m_1, 1, k_1) avec $k_1 = m_1^2 - d$. Ainsi $a_1 = m_1$ et $b_1 = 1$. Pourquoi avoir fait cela ? Il s'agit de commencer par prendre b_1 le plus petit possible, puisque l'on

[19] Il est entendu que le résultat de l'étape 1 peut se déduire de celui de l'étape 0 en appliquant la règle de passage d'une étape à la suivante que nous expliciterons dans ce qui suit. Pour l'étape 0, on a le triplet (1, 0, 1) et m_0 peut être pris quelconque, ce qui nous permet de choisir m_0 tel que m_0^2 soit le plus près de d possible, d'où $m_1 = m_0$ puisque la seule contrainte sur m_1 est que m_1^2 soit le plus près de d..

recherche la première solution, et cela étant fait, d'obtenir une valeur k_1 la plus petite possible. Avec un peu de chance on peut ainsi trouver la première solution. Par exemple, pour $d = 3$, on trouve aussitôt (2, 1, 1). Et si l'on tombe sur $k_1 = -1$ ou ± 2 ou ± 4, on pourra utiliser le raccourci de Brahmagupta pour trouver la solution. Mais on ne le fera pas pour le moment, afin de bien voir le caractère cyclique de la méthode *chakravala*.

Comment passer d'une étape à la suivante ?

Etant arrivé à l'étape *j*, nous commençons par prendre m_j tel que $a_{j-1} + b_{j-1}\, m_j$ soit un multiple de k_{j-1}.[20] Et parmi les m_j positifs trouvés, tous espacés de $|k_{j-1}|$, nous choisissons celui tel que m_j^2 soit le plus proche de *d* possible. Ce choix étant fait, on compose le triplet $(a_{j-1}, b_{j-1}, k_{j-1})$ trouvé à l'étape précédente, avec le triplet $(m_j, 1, m_j^2 - d)$, ce qui donne :

$$(a_{j-1}\, m_j + b_{j-1}\, d,\ \ a_{j-1} + b_{j-1}\, m_j\,;\ \ k_{j-1}\,(m_j^2 - d))$$

Mais grâce au choix de m_j, on sait déjà que $a_{j-1} + b_{j-1}\, m_j$ est divisible par k_{j-1}. Mieux encore, on constate alors que $a_{j-1}\, m_j + b_{j-1}\, d$ et $m_j^2 - d$ sont eux aussi divisibles par k_{j-1}. En divisant les deux membres de l'équation par k_{j-1}^2, on obtient la solution entière :

$$\left(\frac{a_{j-1}m_j + b_{j-1}d}{|k_{j-1}|}, \frac{a_{j-1} + b_{j-1}m_j}{|k_{j-1}|}, \frac{m_j^2 - d}{k_{j-1}}\right)$$

En résumé, l'algorithme fait jouer les relations de récurrence :

Avec m_j tel que $a_{j-1} + b_{j-1}\, m_j = 0\ \ [k_{j-1}]$ et m_j^2 le plus proche de *d*,

$$a_j = \frac{a_{j-1}m_j + b_{j-1}d}{|k_{j-1}|},\ \ b_j = \frac{a_{j-1} + b_{j-1}m_j}{|k_{j-1}|},\ \ k_j = \frac{m_j^2 - d}{k_{j-1}} \quad \text{liés par } a_j^2 - b_j^2 d = k_j$$

avec a_j et b_j premiers entre eux, ainsi que b_j et k_j

6.2.2. Exemples d'application de l'algorithme

- $d = 19$

Etape 1 : $\boldsymbol{m_1 = 4}$ et **(4, 1, -3)**.
Etape 2 : m_2 tel que $4 + m_2 = 0$ [3], soit $m_2 = 2$ [3], et m_2^2 le plus proche de 19, soit $\boldsymbol{m_2 = 5}$.
Puis on compose (4, 1, -3) et (5, 1, 6), d'où (39, 9, -3×6) et on divise les deux membres de l'équation par 3^2 (*a* et *b* divisés par 3, et *k* par 3^2), d'où **(13, 3, -2)**.
Etape 3 : m_3 tel que $13 + 3\, m_3 = 0$ [2], soit $m_2 = 1$ [2], et m_3^2 le plus proche de 19, soit $\boldsymbol{m_3 = 5}$.
On compose (13, 3, -2) et (5, 1, 6), d'où (122, 28, -2×6) et on divise par 2^2, d'où **(61, 14, -3)**.
Etape 4 : m_4 tel que $61 + 14\, m_4 = 0$ [3], soit $m_4 = 1$ [3], et m_4^2 le plus proche de 19, soit $\boldsymbol{m_4 = 4}$.
On compose (61, 14, -3) et (4, 1, -3), d'où (510, 117, -3×-3) et on divise par 3^2, d'où **(170, 39, 1)**.

Remarquons que la suite de (*k*) est 1, -3, -2, -3, 1, où l'on est parti de 1 à l'étape 0.

- $d = 103$

Etape 1 : $\boldsymbol{m_1 = 10}$ et **(10, 1, -3)**.
Etape 2 : $m_2 = -10$ [3] et m_2^2 le plus proche de 103, soit $\boldsymbol{m_2 = 11}$.
Composons (10, 1, -3) et (11, 1, 18), d'où (213, 21, -3×18) et on divise par 3^2, d'où **(71, 7, -6)**.
Etape 3 : m_3 tel que $71 + 7m_3 = 0$ [6], $m_3 = 1$ [6] et m_3^2 le plus proche de 103, soit $\boldsymbol{m_3 = 7}$.
On compose (71, 7, -6) et (7, 1, -54), d'où (1218, 120, 6×54) et on divise par 6^2, d'où **(203, 20, 9)**.
Etape 4 : m_4 tel que $203 + 20m_4 = 0$ [9], $m_4 = 2$ [9], et m_4^2 le plus proche de 103, soit $\boldsymbol{m_4 = 11}$.
On compose (203, 20, 9) et (11, 1, 18), d'où (4293, 423, 9×18) et on divise par 9^2, d'où **(477, 47, 2)**.

On pourrait continuer au-delà de α_4, mais profitons de $k_4 = 2$. On sait alors que le résultat final est $\alpha_4^2 / 2 = 227\,528 + 22\,419\sqrt{103}$. C'est ainsi que procéda Narayana (14è siècle) lorsqu'il annota le *Siddhanta Siroman* de Bhaskara II.

La suite des (*k*) est 1, -3, -6, 9, 2, 9, -6, -3, 1 en allant jusqu'à la fin du premier cycle.

- $d = 97$

Etape 1 : $\boldsymbol{m_1 = 10}$ et **(10, 1, 3)**.

---

[20] On montrera que a_j et b_j sont toujours premiers entre eux, et l'on en déduit que k_j est aussi premier avec b_j (et a_j). Dans ces conditions, avec $a_{j-1} + b_{j-1}\, m_j = 0\ [k_{j-1}]$, $m_j = -\, b_{j-1}^{-1}\, a_{j-1}\ [k_{j-1}]$, et l'on a bien une infinité de valeurs de m_j, une seule (voire deux) étant telle que son carré soit le plus proche de *d* possible.

Etape 2 : m_2 tel que $10 + m_2 = 0$ [3], $m_2 = 2$ [3] et m_2^2 le plus proche de 97, soit $\boldsymbol{m_2} = \mathbf{11}$.
Composons (10, 1, 3) et (11, 1, 24), d'où (207, 21, 3 . 24) et on divise par 3^2, d'où **(69, 7, 8)**.
Etape 3 : m_3 tel que $69 + 7m_3 = 0$, $m_3 = 5$ [8] et m_3^2 le plus proche de 97, soit $\boldsymbol{m_3} = \mathbf{13}$.[21]
On compose (69, 7, 8) et (13, 1, 72), d'où (1576, 160, 8 . 72) et on divise par 8^2, d'où **(197, 20, 9)**.
Etape 4 : m_4 tel que $197 + 20m_4 = 0$ [9], $m_4 = 5$ [9] et m_4^2 le plus proche de 97, soit $\boldsymbol{m_4} = \mathbf{5}$.
On compose (197, 20, 9) et (5, 1, -72), d'où (2925, 297, 9 $\times$ -72) et on divise par 9^2, d'où **(325, 33, -8)**.
Etape 5 : m_5 tel que $325 + 33m_5 = 0$ [8], $m_5 = 3$ [8], et m_5^2 le plus proche de 97, soit $\boldsymbol{m_5} = \mathbf{11}$.
On compose (325, 33, -8) et (11, 1, 24), d'où (6776, 688, -8 $\times$ 24) et on divise par 8^2, d'où **(847, 86, -3)**.
Etape 6 : m_6 tel que $847 + 86m_6 = 0$ [3], $m_6 = 1$ [3] et m_6^2 le plus proche de 97, soit $\boldsymbol{m_5} = \mathbf{10}$.
On compose (847, 86, -3) et (10, 1, 3), d'où (16812, 1707, -3 $\times$ 3) et on divise par 3^2, d'où **(5604, 569, -1)**.

A ce stade, en appliquant la méthode de Brahmagupta ainsi que l'a aussi fait Narayana sur cet exemple, on arrive au résultat final :

$\alpha_{12} = 62\ 809\ 633 + 6\ 377\ 352\ \sqrt{97}$

La suite des (k) est : 1, 3, 8, 9, -8, -3, -1, -3, -8, 9, 8, 3, 1.

• $\boldsymbol{d} = \mathbf{13}$
-étape 1 : $m_1 = 4$ et le triplet (4, 1, 3). Puis, en appliquant les formules, on trouve :
-étape 2 : $m_2 = 2$, et le triplet (7, 2 ; –3)
-étape 3 : $m_3 = 4$, et le triplet (18, 5 ; –1)
-étape 4 : $m_4 = 4$, et le triplet (137, 38 ; –3)
-étape 5 : $m_5 = 2$, et le triplet (256, 71 ; 3)
-étape 6 : $m_6 = 4$, et le triplet (649,180 ; 1), d'où la solution (a, b) = (649, 180).
Vérifions le caractère cyclique de la méthode : Si l'on continue sur les six étapes suivantes, on retrouve le même cycle pour les k_j : 3, –3, –1, –3, 3, 1, ce qui donne une deuxième solution (a, b) = (842 401, 133 640).

• $\boldsymbol{d} = \mathbf{106}$
On trouve comme succession des k_i à partir du rang 0 :
1, –6, 7, 9, – 9, –7, 6, –1, 6, –7, –9, 9, 7, –6, 1, et l'on aboutit à la solution :
a = 32 080 051, b = 3 115 890.

Remarque : On constate que l'on a toujours $m_2 = -\ m_1\ [k_1]$. Nous verrons que cela se généralise à un rang quelconque. Cette formule facilite les calculs, et aussi la démonstration des formules à un rang quelconque.

6.2.3. Démonstrations

Faisons un raisonnement par récurrence pour démontrer les formules encadrées ci-dessus. Les formules sont vraies à l'étape 1. Supposons qu'elles soient vraies jusqu'à un certain rang j, et montrons qu'elles restent vraies au rang $j + 1$.

● m_{j+1} existe. En effet, en prenant les nombres m tels que $a_j + m\, b_j = 0\ [k_j]$, $m\, b_j = -\ a_j\ [k_j]$, $m = -\ a_j\, b_j^{-1}\ [k_j]$, car avec b_j premier avec k_j, l'inverse de b_j existe (c'est une conséquence de l'algorithme d'Euclide). Parmi l'infinité des m obtenus, on choisit m_{j+1} positif et m_{j+1}^2 le plus proche de d possible. On a non seulement $a_j + m_{j+1}\, b_j = 0\ [k_j]$, mais aussi :

● $m_{j+1} = -\ m_j\ [k_j]$
Formons $a_j - b_j\, m_j = \dfrac{a_{j-1}m_j + b_{j-1}d}{|k_{j-1}|} - \dfrac{a_{j-1} + b_{j-1}m_j}{|k_{j-1}|}m_j = -\dfrac{b_{j-1}(m_j^2 - d)}{|k_{j-1}|} = -\dfrac{b_{j-1}k_jk_{j-1}}{|k_{j-1}|} = b_{j-1}k_j$
au signe près
$= 0\ [k_j]$.

Combinons ce résultat avec $a_j + m_{j+1}\, b_j = 0\ [k_j]$, par soustraction :
$b_j\,(m_{j+1} + m_j) = 0\ [k_j]$, et comme b_j est premier avec k_j (ou inversible modulo k_j), $m_{j+1} + m_j = 0\ [k_j]$.

● b_{j+1} est un entier naturel : c'est la conséquence immédiate de ce qui précède, puisque $a_j + m_{j+1}\, b_j = 0\ [k_j]$, la division de $a_j + m_{j+1}\, b_j$ par k_j tombe juste.

● a_{j+1} est un entier naturel :

[21] On pourrait aussi prendre $m_3 = 5$, avec $m_3^2 - 97 = -72$. On obtient alors le triplet (128, 13, -9). En continuant, on trouve $m_4 = 4$ [9] puis $m_4 = 13$. En composant (128, 13, -9) avec (13, 1, 72), on arrive à (2925, 297, -9 $\times$ 72) et après division, on retrouve (325, 33, -8), comme par l'autre méthode.

$a_j m_{j+1} + b_j d = -a_j m_j + b_j d \ [k_j]$

$= -\dfrac{a_{j-1} m_j + b_{j-1} d}{|k_{j-1}|} m_j + \dfrac{a_{j-1} + b_{j-1} m_j}{|k_{j-1}|} d = -\dfrac{a_{j-1}(m_j^2 - d)}{|k_{j-1}|} = -\dfrac{a_{j-1} k_j k_{j-1}}{|k_{j-1}|} \ [k_j]$

$= a_{j-1} k_j = 0 \ [k_j]$

$a_{j+1} = \dfrac{a_j m_{j+1} + b_j d}{|k_j|}$ est bien un entier.

● k_{j+1} est un entier (positif ou négatif) :

$m_{j+1}^2 - d = m_j^2 - d \ [k_j] = k_j k_{j-1} = 0 \ [k_j]$

$k_{j+1} = \dfrac{m_{j+1}^2 - d}{k_j}$ est bien un entier.

● $a_{j+1}^2 - b_{j+1}^2 d = k_{j+1}$: ce résultat est aussitôt obtenu en composant (a_j, b_j, k_j) et (m_{j+1}, 1, $m_{j+1}^2 - d$)

● a_{j+1} et b_{j+1} sont premiers entre eux :

Formons $a_j\, b_{j+1} - b_j\, a_{j+1} = \dfrac{a_j(a_j + b_j m_{j+1}) - b_j(a_j m_{j+1} + b_j d)}{|k_j|} = \dfrac{a_j^2 - b_j^2 d}{|k_j|} = \dfrac{k_j}{|k_j|} = \pm 1$.

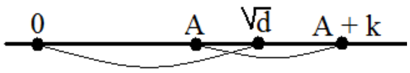
Grâce à Bézout, cela prouve que a_{j+1} et b_{j+1} sont premiers entre eux.

● b_{j+1} et k_{j+1} sont premiers entre eux : avec $a_{j+1}^2 - b_{j+1}^2 d = k_{j+1}$, si b_{j+1} et k_{j+1} n'étaient pas premiers entre eux, ils auraient un diviseur commun autre que 1 qui diviserait a_{j+1}^2 et par suite a_{j+1}, ce qui contredit le fait que a_{j+1} et b_{j+1} sont premiers entre eux.

6.2.4. Efficacité de la méthode, grâce à la majoration $|k_j| < \sqrt{d}$

Au fil des étapes, les valeurs a_j et b_j augmentent, tandis que les $|k_j|$ restent majorés, plus prrécisément $|k_j| < \sqrt{d}$. C'est un bon indicateur de l'efficacité de la méthode.

Montrons que $|k_j| < \sqrt{d}$ par récurrence.[22] C'est vrai au départ. Supposons que cela soit vrai au rang j et montrons que cela reste vrai au rang $j + 1$. On sait que m_{j+1} est à prendre parmi des nombres espacés de $|k_j|$. Parmi ces nombres, il en existe un, noté A qui est positif et inférieur à $\sqrt{d}$, le suivant $A + |k_j|$ étant supérieur à $\sqrt{d}$. En faisant cela nous utilisons l'hypothèse de récurrence, car si l'on avait $k > \sqrt{d}$ on ne serait pas sûr de trouver un tel nombre A.



Dans ces conditions, avec m_{j+1}^2 le plus proche de d possible, m_{j+1} est soit A soit $A + |k_j|$. Pour simplifier nous noterons m pour m_{j+1}, et k pour $|k_j|$. On distingue deux cas :

* premier cas : $m = A$, cela signifie que $d - A^2$ est inférieur à $(A+ k)^2 - d$, ce qui s'écrit :
$2 A^2 + 2kA + k^2 - 2d > 0$, ou $A^2 + kA + k^2/2 - d > 0$.

Considérons la fonction $f(X) = X^2 + kX + k^2/2 - d$ représentée par une parabole tournée vers le haut. L'équation $f(X) = 0$ a pour discriminant $- k^2 + 4d$ qui est positif puisque $k^2 < d$ par hypothèse de récurrence. Elle admet deux solutions dont une seule est positive, soit

$x_0 = (-k + \sqrt{4d - k^2}) / 2 = -k/2 + \sqrt{d - k^2/4}$ (elle est bien positive car le produit des racines est $k^2/2 - d$ qui est négatif puisque $k^2 < d$). $f(X)$ étant négatif entre les racines et positif ailleurs, $f(A)$ positif équivaut à $A > x_0$, ou $m > x_0$, $m^2 > x_0^2$,

$d - m^2 < d - x_0^2$

$< d - (-k/2 + \sqrt{d - k^2/4})^2$

$< k\sqrt{d - k^2/4}$

On sait que $k_{j+1} = (m_{j+1}^2 - d) / k_j$, $|k_{j+1}| = (d - m^2) / k$ avec nos notations.

$|k_{j+1}| < \sqrt{d - k^2/4} < \sqrt{d}$

[22] Cette démonstration est reprise du document *Wikipedia* sur la méthode *chakravala*.

* deuxième cas : $m = A + k$, ce qui signifie que $(A+k)^2 - d$ est inférieur à $d - A^2$, soit :
$A^2 + kA + k^2/2 - d < 0$, et $A < x_0$, ou $A + k < x_0 + k$,
$m < x_0 + k$
$m < k/2 + \sqrt{d - k^2/4}$
$m^2 - d < k\sqrt{d - k^2/4}$ comme dans le premier cas, d'où $|k_{j+1}| < \sqrt{d - k^2/4} < \sqrt{d}$ dans ce cas aussi.

Les k_j restent donc dans un domaine borné, sans que cela prouve que l'on va retomber sur la valeur 1, celle que l'on avait au rang 0. Mais on est sûr que l'on aura à un moment $k_j = \pm k_{j'}$. En prouvant que $k_{j-1} = \pm k_{j'+1}$, et ainsi de suite en reculant d'un côté et en avançant de l'autre, on serait assuré que l'on arrive bien à 1 (ou – 1), et par la même occasion, on saurait que le cycle a l'allure d'un palindrome.

Exemple : $d = 313$. La suite (k) est :

1 11 -8 3 16 -9 **<u>13 -13</u>** 9 -16 -3 8 **-11** -1 **-11** 8 -3 -16 9 -13 13 -9 16 3 -8 11 1

Remarque : dans l'exemple $d = 313$ précédent, on constate que $k_6 = -k_7 = 13$. Connaissant $a_6 = 19\,001$, $b_6 = 1074$, et $a_7 = 43\,398$, $b_7 = 2453$, la composition de ces deux triplets donne $(A, B, -13 \times 13)$ et l'on constate que A et B sont divisibles par 13, ce qui donne après division le triplet (126 862 368, 7 170 685, -1). C'est alors quasiment fini.

6.2.5. Simplification des calculs

1) Calcul des m_j et k_j indépendamment des a_j et b_j

Le fait d'avoir $m_{j+1} = -m_j\ [k_j]$ et $k_{j+1} = \dfrac{m_{j+1}^2 - d}{k_j}$ à partir de $m_0 = 1$ et $k_0 = 1$, permet de calculer la suite des (m) et des (k) sans avoir besoin des suites (a) et (b).Par la même occasion, on peut calculer la suite (q) définie par $m_j + m_{j+1} = q_{j+1}|k_j|$. Cela va nous servir dans ce qui suit.

2) Relation de récurrence du second ordre pour les a_j et les b_j

A partir de $a_0 = 1$, $a_1 = m_1$, $b_0 = 0$, $b_1 = 1$, on a les relations de récurrence :

$a_{j+2} = q_{j+2}\, a_{j+1} \pm a_j$
$b_{j+2} = q_{j+2}\, b_{j+1} \pm b_j$
avec le signe + si $k_j \times k_{j+1} < 0$ et – si $k_j \times k_{j+1} > 0$

Démonstration :
$a_{j+2} = (a_{j+1} m_{j+2} + b_{j+1} d)/|k_{j+1}| = (a_{j+1}(m_{j+2} + m_{j+1}) - a_{j+1} m_{j+1} + b_{j+1} d)/|k_{j+1}|$
$= (a_{j+1} q_{j+2} |k_{j+1}| - a_{j+1} m_{j+1} + b_{j+1} d)/|k_{j+1}| = a_{j+1} q_{j+2} + X$ avec $X = -a_{j+1} m_{j+1} + b_{j+1} d)/|k_{j+1}|$

$|k_{j+1}|\,|k_j|\,X = -|k_j|\, a_{j+1} m_{j+1} + |k_j|\, b_{j+1} d = -m_{j+1}(a_j m_{j+1} + b_j d) + (a_j + b_j m_{j+1}) d = -a_j m_{j+1}^2 + a_j b_j d$
$= -a_j (m_{j+1}^2 - d) = -a_j k_{j+1} k_j$
$X = -\text{signe}(k_{j+1} k_j)\, a_j$
Finalement $a_{j+2} = a_{j+1} q_{j+2} - \text{signe}(k_{j+1} k_j)\, a_j$.
On ferait de même pour b_{j+2}.

Exemple : $d = 13$

On commence par calculer les suites (m), (k), (q) grâce au 1°.
étape 0 : $m_0 = 4$, $k_0 = 1$ (mais pour q_1 on doit prendre $m_0 = 1$)
étape 1 : $m_1 = 4$, $k_1 = 3$, $q_1 = 5$
étape 2 : $m_2 = 2$, $k_2 = -3$, $q_2 = 2$
étape 3 : $m_3 = 4$, $k_3 = -1$, $q_3 = 2$
étape 4 : $m_4 = 4$, $k_4 = -3$, $q_4 = 8$
étape 5 : $m_5 = 2$, $k_5 = 3$, $q_5 = 2$
étape 6 : $m_6 = 4$, $k_6 = 1$, $q_6 = 2$

Puis on passe aux suites (a) et (b) grâce au 2°
étape 0 : $a_0 = 1$, $b_0 = 0$
étape 1 : $a_1 = 4$, $b_1 = 1$
étape 2 : $a_2 = 2 \times 4 - 1 = 7$, $b_2 = 2 \times 1 - 0 = 2$
étape 3 : $a_3 = 2 \times 7 + 4 = 18$, $b_3 = 2 \times 2 + 1 = 5$
étape 4 : $a_4 = 8 \times 18 - 7 = 137$, $b_4 = 8 \times 5 - 2 = 38$
étape 5 : $a_5 = 2 \times 137 - 18 = 256$, $b_5 = 2 \times 38 - 5 = 71$
étape 6 : $a_6 = 2 \times 256 + 137 = 649$, $b_6 = 2 \times 71 + 38 = 180$

3) Raccourci pour les calculs si l'on tombe à un certain rang sur $k_{j+1} = \pm k_j$

Remarquons-le d'abord sur l'exemple précédemment donné avec $d = 313$: on constate que $k_6 = - k_7 = 13$. Connaissant $a_6 = 19\,001$, $b_6 = 1074$, et $a_7 = 43\,398$, $b_7 = 2453$, la composition de ces deux triplets donne (A, B , -13×13) et l'on constate que A et B sont divisibles par 13, ce qui donne après division le triplet (126 862 368, 7 170 685, -1).

Démonstration :

Supposons que l'on ait, à une certaine étape j :
$a_j^2 - b_j^2 d = k_j$ et $a_{j+1}^2 - b_{j+1}^2 d = k_{j+1}$ avec $|k_{j+1}| = |k_j|$.

Par composition, on trouve le triplet :
($A = a_j a_{j+1} + b_j b_{j+1} d$, $B = a_j b_{j+1} + b_j a_{j+1}$, $\pm k_j^2$)

On sait que $a_{j+1} - m_{j+1} b_{j+1} = 0$ $[k_{j+1}]$, ou $a_{j+1} = m_{j+1} b_{j+1}$ $[k_{j+1}]$ ou $[k_j]$
Alors, modulo k_j :
$A = a_j m_{j+1} b_{j+1} + b_j b_{j+1} d = b_{j+1} (a_j m_{j+1} + b_j d) = 0$ $[k_j]$ car $|k_j|$ divise $a_j m_{j+1} + b_j d$ pour donner a_{j+1}.
$B = a_j b_{j+1} + b_j m_{j+1} b_{j+1} = b_{j+1} (a_j + b_j m_{j+1}) = 0$ $[k_j]$ car $|k_j|$ divise $a_j + b_j m_{j+1}$ pour donner b_{j+1}.

En divisant les deux membres de l'équation par k_j^2, on trouve ($A / |k_j|$, $B / |k_j|$, ± 1).

4) Raccourci si l'on tombe sur $k_{j+2} = k_j$

La relation de récurrence sur les k_j donne :
$k_j k_{j+1} = m_{j+1}^2 - d$ et $k_{j+1} k_{j+2} = m_{j+2}^2 - d$. Avec $k_{j+2} = k_j$, on obtient $m_{j+2} = m_{j+1}$.
Composons les triplet (a_j, b_j, k_j) et (a_{j+2}, b_{j+2}, k_j), ce qui donne le triplet :
($A = a_j a_{j+2} + b_j b_{j+2} d$, $B = a_j b_{j+2} + b_j a_{j+2}$, k_j^2)

Utilisons $a_{j+2} = m_{j+2} b_{j+2}$ $[k_{j+2}]$ ou encore $[k_j]$. En se ramenant modulo k_j
$A = a_j a_{j+2} + b_j b_{j+2} d = a_j m_{j+2} b_{j+2} + b_j b_{j+2} d = b_{j+2} (a_j m_{j+2} + b_j d) = b_{j+2} (a_j m_{j+1} + b_j d) = 0$ $[k_j]$ grâce à la formule sur a_{j+1}.

$B = a_j b_{j+2} + b_j a_{j+2} = a_j b_{j+2} + b_j m_{j+2} b_{j+2}$ $[k_j]$
$= b_{j+2} (a_j + b_j m_{j+2}) = b_{j+2} (a_j + b_j m_{j+1}) = 0$ $[k_j]$ grâce à la formule sur b_{j+1}.

En divisant l'équation par k_j^2 (et donc A et B par $|k_j|$),on obtient le triplet correspondant à la solution primitive de l'équation de Pell.

***Exemple* : *d* = 207**
étape 1 : $m = 14$, $k = - 11$, $a = 14$, $b = 1$
étape 2 : $m = 8$, $k = 13$, $a = 29$, $b = 2$
étape 3 : $m = 18$, $k = 9$, $a = 72$, $b = 5$
étape 4 : $m = 18$, $k = 13$, $a = 259$, $b = 18$

On est dans les conditions où $k_2 = k_4$. En composant (29, 2, 13) et (259, 18, 13) puis en divisant par 13^2, on trouve la solution (1151, 80, 1), ce qui correspond à l'étape 6 de la méthode *chakravala*.

Cela étant dit, il arrive souvent que l'on ait la succession des trois valeurs : k_j , – 1, k_{j+2} avec $k_{j+2} = k_j$, et dans ce cas le fait de tomber sur -1 permet d'appliquer la méthode de Brahmagupta sans avoir à chercher k_{j+2}.

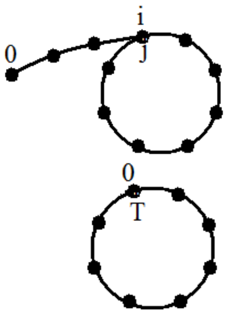
6.2.6. Caractère cyclique et palindromique de la méthode

Nous savons déjà que $|k_j| < \sqrt{d}$. Cela étant, on en déduit, grâce à $k_j k_{j+1} = m_{j+1}^2 - d$, que
$m_{j+1}^2 = k_j k_{j+1} + d$.
Avec $-d < k_j k_{j+1} < d$, on a alors $0 < m_j^2 < 2d$. Finalement, sachant que m_j est positif, $0 < m_j < \sqrt{2d}$. Les termes des suites (k) et (m) sont bornées, ainsi que ceux de la double suite (m, k), où nous profitons du fait que l'on peut calculer les (m_j, k_j) indépendamment des valeurs de a_j et b_j.

Voyons cela sur l'exemple de $d = 61$, avec cette évolution de la suite (m, k) à partir de (m_0, k_0) :

(8, 1), (8, 3), (7, -4), (9, -5), (8, 1), (6, 5), (9, 4), (7, -3), (8, -1), (8, -3), (8, 1), (7, 4), (9, 5), (6, -5), (9, -4), (7, 3), (8, 1), (8, 3), ...

Comme la suite (m, k) ne peut prendre qu'un nombre fini de valeurs, elle va forcément repasser là où elle est déjà passée, et elle présente cette forme, avec un premier retour où $(m_j, k_j) = (m_i, k_i)$, $j > i$:



Mais le passage d'un terme au suivant est bijectif. On passe en effet du terme (m_{j+1}, k_{j+1}) à (m_j, k_j) en faisant :

$k_j = \frac{m_{j+1}^2}{k_{j+1}}$ puis $m_j = -m_{j+1}\ [k_j]$ avec m_j^2 le plus proche de d.

Dans ces conditions, le dessin précédent n'est plus valable, m_j ayant deux antécédents. La seule possibilité est le retour à 0. Il existe un nombre T où pour la première fois (m_T, k_T) = (m_0, k_0).

La suite (m, k) est périodique, sa plus petite période étant T. On obtient toutes les solutions de l'équation de Pell en prenant (m_{kT}, 1) avec $k > 0$.

D'autre part, comme $m_1 = m_0$, on a aussi (m_1, k_0) = (m_T, k_T). En avançant d'un cran à partir de (m_1, k_0), on a (m_2, k_1) avec $m_2 = - m_1\ [k_1]$ et $k_1 = \frac{m_1^2 - d}{k_0}$.

En reculant d'un cran à partir de (m_T, k_T), on a (m_{T-1}, k_{T-1}) avec $k_{T-1} = \frac{m_T^2 - d}{k_T} = \frac{m_1^2 - d}{k_0} = k_1$ et $m_{T-1} = -m_T\ [k_{T-1}] = -m_1\ [k_1] = m_2$. D'où ($m_2$, k_1) = (m_{T-1}, k_{T-1}).

Pour les mêmes raisons : (m_3, k_2) = (m_{T-2}, k_{T-2}), (m_4, k_3) = (m_{T-3}, k_{T-3}), ..., (m_{i+1}, k_i) = (m_{T-i}, k_{T-i}),[23] et cela jusqu'à la rencontre des termes qui avancent et de ceux qui reculent. On a bien un palindrome de longueur $T + 1$, entre les étapes 0 et T, pour la suite (k) et un palindrome entre les étapes 1 et T (ou entre 0 et $T + 1$) pour la suite (m).

Exemple : $d = 13$

étape	*m*	*k*
0	4	**1**
1	4	**3**
2	2	**-3**
3	4	**-1**
4	4	**-3**
5	2	**3**
6	4	**<u>1</u>**
7	4	3
8	2	-3

6.2.7. De l'Inde à l'Europe

A leur époque, les mathématiciens indiens ont fait avant tout une étude expérimentale, mais ils ont trouvé la méthode de composition qu'Euler appellera plus tard le « théorème élégantissime », et ils connaissaient l'algorithme d'Euclide qui leur permettait d'être assurés que les m_j existent dans la méthode cyclique. Un millier d'années plus tard, au 17è siècle, plusieurs mathématiciens européens reprennent le problème, sous l'impulsion de Fermat en 1657. Ils ne donnent pas plus de preuve que leurs prédécesseurs indiens. Ces mathématiciens s'appellent notamment Frénicle de Bessy, Wallis, Brouncker, voire Pell, et Euler par la suite qui fera une démonstration partielle.

6.3. Méthode anglaise et méthode indienne

Selon les sources, J. Wallis se voit attribuer deux méthodes, la première étant originale, tandis que ce que l'on appelle la « méthode anglaise », où le nom de Wallis est associé à celui de W. Brouncker,[24] est proche de celle des Indiens.

---

[23] Prouvons-le en faisant un raisonnement par récurrence : en supposant que $k_{T-j} = k_j$ et $m_{T-j} = m_{j+1}$ à un rang j, montrons qu'il en est de même au rang suivant :

$$k_{T-j-1} = \frac{m_{T-j}^2 - d}{k_{T-j}} = \frac{m_2^{j+1} - d}{k_j} = k_{j+1}$$

$$m_{T-j-1} = -m_{T-j}\ [k_{T-j}] = -m_j\ [k_j] = m_{j+1}$$

Les égalités se propagent en descente d'un côté et en montée de l'autre.

[24] Les mauvaises langues affirment que J. Wallis aurait attribué sa propre contribution à W. Brouncker car ce dernier était président de la *Royal Society* en 1660.

6.3.1. Une méthode de Wallis

La méthode qui suit est attribuée à J. Wallis dans [BAR2003]. A partir de l'équation $x^2 - d\ y^2 = 1$, il s'agit de déterminer le nombre *c* dont le carré est juste au-dessus de *d*, et l'on pose $c^2 - d = k$. Exceptionnellement, si $k = 1$, on a le triplet (*c* , 1, 1), et c'est fini. Sinon, multiplions $c^2 - d = k$ par un nombre positif *m* au carré, soit

$(cm)^2 - dm^2 = km^2$, ce qui entraîne $dm^2 < (cm)^2$.

Lorsque *m* augmente à partir de 1, l'écart entre les deux membres de l'inégalité augmente (c'est km^2). Il est alors sûr qu'à un certain moment, on tombera pour la première fois sur $dm^2 < (cm - 1)^2$, ou encore $d\,m^2 \le (c\,m-1)^2 - 1$. Deux cas sont possibles :

$d\,m^2 = (c\,m-1)^2 - 1$, et c'est fini, avec la solution $(cm - 1, m)$

ou $d\,m^2 < (c\,m-1)^2 - 1$.

Dans ce deuxième cas, on continue d'augmenter *m* jusqu'à ce que l'on tombe sur :

$d\,m^2 \le (c\,m-2)^2 - 1$. Là encore deux cas se présentent, et si ce n'est pas fini, on continue d'augmenter *m* jusqu'à tomber sur $d\,m^2 \le (c\,m-3)^2 - 1$. Et ainsi de suite, où *m* augmente pas à pas, tandis qu'une deuxième variable *i* augmente de temps à autre, comme ici pour $i = 3$. On finira par tomber sur :

$d\,m^2 = (c\,m - J)^2 - 1$ avec $i = J$, soit la solution $(cm - J, m)$ qui est la solution primitive.

Le nombre d'étapes de calcul est le *m* final, avec $Y = m$. Cette méthode exhaustive ne peut marcher que si la solution primitve est formée de petits nombres. Elle est beaucoup plus longue que la méthode Brahmagupta-Bhaskara II. Par contre l'algorithme sur ordinateur est particulièrement simple, et si l'on est patient –si l'on daigne attendre une seconde ou deux pour avoir le résultat, on pourrra retrouver la solution pour $d = 61$.

```
double d = 51.;
int main()
{ double m,i,c;
  c=1;
  while(c*c<d) c++;  /* calcul de c */
  if (c*c-d==1) { printf("\n\n  *** %3.f  1  *** ", c);  getchar();return 0;}
  i=1; m=0;
  for(;;)
    { m++;  /* m augmente au coup par coup */
      printf(" (%1.f  %1.f)", m,i); /* affichage des valeurs de m et i, ce qui est facultatif */
      if ((c*m-i)*(c*m-i)-d*m*m==1) break;
      if ((c*m-i)*(c*m-i)-d*m*m>1)  i++;  /* dans ce cas i augmente de 1 */
    }
 printf("\n\n  *** %3.f  %3.f ***", c*m-i, m);  getchar();return 0;
}
```

Prenons un exemple : $d = 51$.
$c = 8$, $k = 13$, et $51m^2 < 8^2\,m^2$
A partir de quand a-t-on $51m^2 \le (8m - 1)^2 - 1$?
Pour $m = 1$, on n'a pas $51 \le 7^2$, mais pour $m = 2$, on a bien $51 \times 4 \le 15^2 - 1$, mais pas =.
Quand a-t-on $51m^2 \le (8m - 2)^2 - 1$? Dès $m = 3$, $51 \times 3^2 \le 22^2 - 1$, mais pas =.
Quand a-t-on $51m^2 \le (8m - 3)^2 - 1$? Dès $m = 4$, $51 \times 4^2 \le 29^2 - 1$, mais pas =.
Quand a-t-on $51m^2 \le (8m - 4)^2 - 1$? Dès $m = 5$, $51 \times 5^2 \le 36^2 - 1$, mais pas =.
Quand a-t-on $51m^2 \le (8m - 5)^2 - 1$? Dès $m = 6$, $51 \times 6^2 \le 43^2 - 1$, mais pas =.
Quand a-t-on $51m^2 \le (8m - 6)^2 - 1$? Dès $m = 7$, $51 \times 7^2 \le 50^2 - 1$, et même $51 \times 7^2 = 50^2 - 1$.
On a trouvé la solution (50, 7).

6.3.2. La méthode anglaise (Wallis-Brouncker)

D'après [EDW1991], la méthode anglaise s'apparente à la méthode indienne, sauf qu'au lieu de prendre *m* dont le carré est le plus proche de *d*, elle prend *m* dont le carré est le plus proche de *d* mais inférieur à lui. On constate alors que les calculs intermédiaires sont les mêmes dans les deux cas, avec seulement quelques étapes supplémentaires pour la méthode anglaise. Après avoir démontré cela, H.M. Edwards en déduit que pour démontrer la méthode indienne, il suffit de démontrer la méthode anglaise qui est un peu plus simple dans ses principes. Et cette démonstration est faite en exercices dans son livre. Nous allons en donner quelques indications, en commençant par un exemple comparatif.

Prenons $d = 61$.

A l'étape 2 du calcul pour la méthode indienne et à l'étape 3 pour la méthode anglaise, les deux méthodes donnent $m = 7$ et $k = -4$.

A l’étape suivante, les deux méthodes divergent :
à l’étape 3, la méthode indienne donne $M = 9$, $K = -5$,
à l’étape 4, la méthode anglaise donne $m' = 5$ et $k' = 9$.

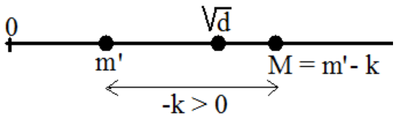
Mais continuons la méthode anglaise : à l’étape 5, elle donne $m'' = 4$ et $k'' = -5$. On retrouve $k'' = K$.
Finalement, à l’étape 4 pour la méthode indienne, et à l’étape 6 pour la méthode indienne, les deux donnent $m''' = M' = 6$ et $k''' = K' = 5$.

Autrement dit, par moments, la méthode anglaise fait en deux étapes ce que la méthode indienne fait en une étape. Il reste à le démontrer, ce que nous allons faire dans le cas où k est < 0, le cas $k > 0$ étant du même style, et nous gardons les mêmes notations que pour notre exemple $d = 61$.

Constatons d’abord que dans les deux méthodes on a toujours :

$m_{j+1} = - m_j$ [kj], la démonstration étant la même pour la méthode anglaise que celle que nous avons faite précédemment.

Partons d’une situation où les deux méthodes ont leur m et leur k (<0) identiques. Mais à l’étape suivante, elles se séparent, avec la situation suivante pour m' et M :



Cela signifie que $d - m'^2 > M^2 - d$
avec $k' = \dfrac{m'^2 - d}{k} > 0$ car $m'^2 - d < 0$.
Encore faut-il que m' existe, c’est-à-dire $m > 0$. Mais on a vu que dans la méthode indienne, $-k = |k| < \sqrt{d}$, donc $m' = M + k > M - \sqrt{d} > (M^2 - d)/(M + \sqrt{d}\,) > 0$.

$$M^2 - d = (m' - k)^2 - d = m'^2 - 2km'' + k^2 - d$$
$$= kk' - 2km' + k^2 = k(k' - 2m' + k)$$

Avec $k < 0$ et $M^2 - d > 0$, $k' - 2m' + k < 0$

A l’étape suivante de la méthode anglaise, on sait déjà que $m'' = - m'$ [k'], soit $m'' = - m' + k'$, ou $m'' = - m' + 2k'$, etc., pourvu que son carré soit inférieur à d. D’abord essayons $-m' + k'$:

$$(-m' + k')^2 - d = m'^2 - 2km' + k'^2 - d$$
$$= kk' - 2km' + k'^2 = k'(k - 2m' + k')$$

On en déduit que :

$$\frac{(-m' + k')^2 - d}{k'} = k - 2m' + k' < 0 \quad \text{d'où} \quad (-m' + k')^2 - d < 0$$

Prenons maintenant $- m' + 2k'$:

$$(-m' + 2k')^2 - d = m'^2 - 4km' + 4k'^2 - d$$
$$= kk' - 4km' + 4k'^2 = k'(k - 4m' + 4k')$$

Or $k - 2m' + 2k' = 2(k - 2m' + k') + k' > 0$ (car $k' > 0$)
et $k - 4m' + 4k' = 2(k - 2m' + 2k') - k > 0$ (car $k < 0$)
Finalement $(-m' + 2k')^2 - d > 0$.
Cela prouve que $m'' = - m' + k'$. Plus généralement on aura $m'' = - m' + |k'|$ que k' soit positif ou négatif.

Mais a-t-on $m'' > 0$? On sait que
$M^2 - d = (m' - k)^2 - d < m'^2 - d$ (toujours avec $k < 0$)
$m'^2 - 2km' + k^2 - d < m'^2 - d$
$m'^2 - d < km' - k^2/2$
$m'^2 - d < k\,(m' - k/2)$
$k' = (m'^2 - d) / k > (m' - k/2) > m'$, d’où $m'' > 0$.

D’autre part, on a vu que $\dfrac{(-m' + k')^2 - d}{k'} = \dfrac{(m + k')^2 - d}{k}$

Or par la méthode anglaise après deux étapes : $k'' = \dfrac{(-m' + k')^2 - d}{k'}$, et par la méthode indienne après une étape :

$K = \dfrac{(m + k')^2 - d}{k}$. Donc $k'' = K$.

Cela ne suffit pas. Encore faut-il que les triplets solutions (A, B, K) pour la méthode indienne et (a'', b'', k'') pour la méthode anglaise soient les mêmes. Montrons que $b'' = B$, ce qui entraînera $a'' = A$.

Avec $a' = \frac{am' + bd}{-k}$ et $b' = \frac{a + bm'}{-k}$,

$$b'' = \frac{a' + b'm''}{k'} = \frac{a' + b'(-m' + k')}{k'} = \frac{am' + bd + (a + bm')(-m' + k')}{-kk'}$$

$$= \frac{ak' + b(d - m'^2 + k'm')}{-kk'} = \frac{ak' + b(kk' + k'm')}{-kk'} = \frac{a + b(k + m')}{-k}$$

On a aussi $B = \frac{a + bM}{-k} = \frac{a + b(m' + k)}{-k} = b''$

Pour que l'étude de la méthode indienne puisse se ramener à celle de la méthode anglaise, encore convient-il que les étapes supplémentaires de cette dernière ne donnent pas une valeur de *k*' égale à 1. C'est justement le cas puisque $m' + m'' = k'$ avec m' et $m'' > 0$. Les deux méthodes tomberont donc en $k = 1$ dans la partie commune de leurs calculs.

A ce stade, nous n'avons pas pour autant démontré que la méthode anglaise aboutit aussi à un cycle avec un retour de *k* en 1. Une démontration est donnée en exercice par Edwards.[25]

Tous les commentateurs européens de la méthode anglaise, des années 1800 à nos jours, affirment que ses auteurs ne connaissaient pas la méthode indienne. Sans aucune preuve. Les commentateurs indiens pourraient, eux, considérer comme plausible qu'elle ait inspiré Brouncker, puisque son traitement de l'équation de Pell est proche de la méthode *chakravala*.[26]

Les Anglais et les Indiens ont au moins quelque chose en commun : ils ont fait essentiellement une étude expérimentale. C'est seulement un siècle après Wallis que Lagrange (1736-1813) donnera une démonstration complète, en utlilisant l'expansion de $\sqrt{d}$ en fractions continuées, comme on va le voir ci-dessous.

6.4. Résolution complète de l'équation de Pell

Voici comment trouver les solutions de l'équation de Pell, comme on peut le lire dans les manuels d'arithmétique d'aujourd'hui. Précisons que la démonstration est assez longue, par exemple le chapitre *fractions continuées* compte 35 pages dans un livre de référence [NIV1991]. Rappelons que l'écriture d'un nombre *A* sous forme de fractions continuées consiste à pratiquer la récurrence suivante, à partir de $x_0 = \sqrt{d}$:

$$x_0 = [x_0] + 1/x_1 \ , \ x_1 = [x_1] + 1/x_2 \ , \ \ldots , x_n = [x_n] + 1/x_{n+1} \ , \ \ldots$$

Faisons maintenant cela pour $\sqrt{d}$, comme par exemple $\sqrt{13}$:

$$\sqrt{13} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \ldots}}}}}$$

ce que l'on écrit plus simplement : $\sqrt{13} = [3,1,1,1,1,6,\ldots]$. On démontre alors que pour un nombre comme $\sqrt{d}$ ($d > 0$ non carré), l'expansion en fractions continuées est périodique à partir d'un certain rang. Par exemple pour $\sqrt{13}$, la période est $\underline{1\ 1\ 1\ 1\ 6}$. On démontre aussi que cette période se termine toujours par le nombre 2 x_0, comme par exemple pour $\sqrt{13}$ où $x_0 = 3$. Et cette période, si on lui enlève son dernier terme, a la forme d'un palindrome comme par exmple pour $\sqrt{13}$ ou $\sqrt{19} = [4,2,1,3,1,2,8]$ avec la période $\underline{2\ 1\ 3\ 1\ 2\ 8}$.

---

[25] Cette démonstration n'est pas particulièrement lumineuse. En fait, il ne semble pas plus simple de démontrer la validité de la méthode anglaise que celle de la méthode indienne. La méthode anglaise a surtout le mérite de donner une alternance de signes + et – pour la suite (*k*), ce qui implique que la période obtenue est toujours paire. Précisons que pour la méthode indienne, une démontration de son caractère cyclique a été faite par K. Ayyangar [AYY1930], et qu'une autre se trouve dans l'article de *Wikipédia* consacré à la méthode *chakravala*. Mais elles ne sont pas très convaincantes, disons que je ne les ai pas biern comprises.

[26] Mais Brouncker innove par rapport à la formule de Madhava (puis de Gregory et Leibniz) d'approximation de $\pi/4$, en remarquant que :

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{\ldots}}}}$$

formule plus tard démontrée par Euler.

En tronquant les fractions à partir du début, on obtient ce que l'on appelle les réduites h_n / k_n qui sont des nombres rationnels. Par exemple, pour $\sqrt{13}$, on trouve :

$$\frac{h_0}{k_0} = 3 = \frac{3}{1}$$

$$\frac{h_1}{k_1} = 3 + \frac{1}{1} = \frac{4}{1}$$

$$\frac{h_2}{k_2} = 3 + \frac{1}{1+\frac{1}{1}} = \frac{7}{2}$$

$$\frac{h_3}{k_3} = 3 + \frac{1}{1+\frac{1}{1+\frac{1}{1}}} = \frac{11}{3}$$

Cela étant connu, on en déduit le théorème donnant toutes les solutions de l'équation de Pell, à partir de sa première solution non évidente, appelée solution primitive, puisqu'elle engendre toutes les autres.

Toutes les solutions positives de l'équation $x^2 - d\ y^2 = \pm 1$ (*d* positif et non carré) se trouvent parmi les réduites h_n / k_n de l'expansion de $\sqrt{d}$ en fractions continuées, en prenant $x = h_n$ et $y = k_n$.

Appelons *T* la période de l'expansion de $\sqrt{d}$.

● Si *T* est un nombre pair, l'équation $x^2 - d\ y^2 = -1$ n'a pas de solution, et toutes les solutions de $x^2 - d\ y^2 = 1$ sont de la forme $x = h_{nT-1}$, $y = k_{nT-1}$ avec *n* entier positif.

● Si *T* est un nombre impair, l'équation $x^2 - d\ y^2 = -1$ a toutes ses solutions de la forme $x = h_{nT-1}$, $y = k_{nT-1}$ avec *n* entier impair positif, et toutes celles de $x^2 - d\ y^2 = 1$ sont de la forme $x = h_{nT-1}$, $y = k_{nT-1}$ avec *n* entier pair positif.

Si (x_1, y_1) est la plus petite solution positive de $x^2 - d\ y^2 = 1$, alors toutes les solutions sont données par (x_n, y_n) avec *n* entier positif, et $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.

6.5. Comparaison des méthodes

Toutes les méthodes utilisent les réduites de fractions continuées de façon explicite ou implicite. On a vu que la méthode indienne était un petit raccourci par rapport à la méthode anglaise. Celle-ci utilise des m^2 inférieur à *d* et le plus près possible. La méthode classique d'aujourd'hui utilise de même des parties entières pour avoir l'expansion de $\sqrt{d}$. On trouve aussi un palindrome dans toutes les méthodes. Mais le mode de calcul et la démonstration de ces méthodes sont foncièrement différents. C'est seulement en 1930 que K. Ayyangar [AYY1930] ose affirmer qu'il est le premier à apporter la preuve de la méthode *chakravala*, contrairement aux bobards affirmant jusque-là -et même après- que c'est Lagrange qui avait prouvé cette méthode.

Dans ce qui suit, nous donnons quelques exemples comparant la méthode par expansion de $\sqrt{d}$ en fractions continuées et la méthode *samasa bhavana - chakravala* de Brahmagupta - Bhaskara II - Narayana[27].

• $n = 31$
Fractions continuées
$\sqrt{31}$ = [5, $\underline{1, 1, 3, 5, 3, 1, 1, 10}$] période 8
réduites : 5/1, 6/1, 11/2, 39/7, 206/37, 657/118, 863/155, **1520/273**, 16063/2885

Méthode chakravala
k : 1, 5, -3, 2, -3, 5, 1 période 6. Pas de -1 : $x^2 - 31\ y^2 = -1$ n'a pas de solution.
6/1, 11/2, 39/7, 206/37, 657/118, **1520/273** . En continuant on a la solution suivante :
4 620 799/829 920.

Méthode samasa bhavana - chakravala
6/1, 11/2, 39/7 avec $k = 2$, d'où la solution primitive **1520/273**.

• $n = 29$
Fractions continuées
$\sqrt{29}$ = [5, $\underline{2, 1, 1, 2, 10}$] période 5.
réduites : 5/1, 11/2, 16/3, 27/5, 70/13, 727/135, d'où la solution primitive **9801/1720**.

[27] On peut associer un quatrième protagoniste, Jayadeva (années 1000).

Méthode chakravala
k : 1, -4, -5, 4, -1, 4, 5, -4, 1 période 8.
5/1, 16/3, 27/5, 70/13, 727/135, 2251/418, 3775/701, **9801/1820**.

Méthode samasa bhavana - chakravala
5/1, 16/3, 27/5 avec $k = 4$, d'où la solution primitive **9801/1820**.

6.6. Quelques problèmes utilisant l'équation de Pell

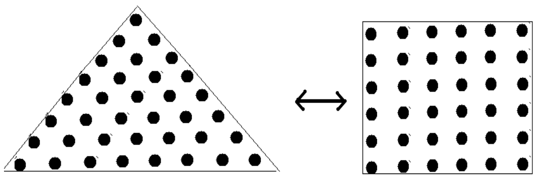
• *Approximation d'une racine carrée*

Avec a et b solutions positives de l'équation de Pell, on a $a^2 - d\, b^2 = 1$ ou $(a + b\sqrt{d})(a - b\sqrt{d}) = 1$, ce qui entraîne $a - b\sqrt{d} > 0$ ou $a > b\sqrt{d}$. Cela permet d'écrire :
$\left|\frac{a}{b} - \sqrt{d}\right| = \frac{a - b\sqrt{d}}{b} = \frac{1}{b(a + b\sqrt{d})} < \frac{1}{b(2b\sqrt{d})} < \frac{1}{2b^2}$. Le fait d'avoir $\left|\frac{a}{b} - \sqrt{d}\right| < \frac{1}{2b^2}$ indique que a/b est nécessairement une réduite dans l'expansion de $\sqrt{d}$ et qu'il s'agit d'une bonne approximaton de $\sqrt{d}$. Il est vraisemblable que les premiers travaux sur l'équation $x^2 - d\ y^2 = 1$ aient été motivés par la volonté de calculer une racine carrée d'un nombre d. Mais rappelons que la méthode de Héron est plus simple et efficace, en pratiquant la récurrence $u_{n+1} = (1/2)(u_n + d / u_n)$ à partir de $u_0 = d/2$.

Il est aussi possible que les pionniers en la matière aient voulu traiter une équation du second degré à deux inconnues avec des solutions entières, le problème du premier degré n'ayant plus de mystère. Et cela d'autant plus que cette équation présentait une infinité de solutions, à la différence d'une équation comme $x^2 + d\ y^2 = k$ qui n'a qu'un nombre fini de solutions.[28]

En fait l'équation $x^2 - d\ y^2 = 1$ intervient dans de nombreux problèmes, comme ceux que nous indiquons ci-dessous.

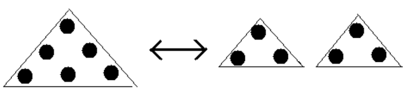
• *On veut transformer un assemblage triangulaire de disques, au nombre de $T_n = 1 + 2 + ... + n$, en un assemblage carré où ces mêmes disques sont au nombre de m^2 ? Si c'est possible, donner quelques solutions.*



n et m doivent vérifier $n\,(n + 1)\,/2 = m^2$
$n^2 + n - 2m^2 = 0$
$(n + 1/2)^2 - 1/4 - 2m^2 = 0$
$(1/4)(2n + 1)^2 - 1/4 - 2m^2 = 0$
$(2n + 1)^2 - 8\,m^2 = 1$, soit $X^2 - 8\,Y^2 = 1$ avec $X = 2n + 1$ et $Y = m$.

$X^2 - 8\,Y^2 = 1$ a pour solution primitive (3, 1). Par composition les suivantes sont (17, 6), (99, 35) ...
On en déduit les couples (n, m) : (1, 1) sans intérêt, puis (8, 6) et (49, 35).

• *Trouver un nombre triangulaire qui est le double d'un autre nombre triangulaire.*



• *Trouver les deux nombres triangulaires les plus petits tels qu'en leur ajoutant 1 on obtienne un carré. Puis déterminer comment en trouver une infinité d'autres.*

On constate aussitôt que $T_2 + 1 = 2^2$ et que $T_5 + 1 = 4^2$. Il s'agit des deux plus petits nombres triangulaires ayant cette propriété. Plus généralement on veut avoir $T_n + 1 = m^2$. Par un calcul analogue à ceux qui précèdent, on arrive à l'équation $X^2 - 8Y^2 = -7$ avec $X = 2n + 1$ et $Y = m$. Les deux solutions particulières trouvées précédemment correspondent à $\alpha = (5, 2)$ et $\alpha' = (11, 4)$. Or la solution primitive de $X^2 - 8Y^2 = 1$ est $\beta = (3, 1)$. En composant $\alpha = (5, 2)$ avec β^k $(k > 0)$, on trouve une

[28] Si l'équation $x^2 - d\ y^2 = 1$ est parfaitement connue, le cas plus général où $x^2 - d\ y^2 = k$ est plus problématique. Il peut y avoir une inifnité de solutions, ou aucune. Par exemple, l'équation $x^2 - 3\ y^2 = 2$ n'a aucune solution (en effet en passant modulo 3, elle devient $x^2 = 2$ [3], qui n'a pas de solution). De même l'équation $x^2 - d\ y^2 = -1$ avec $d = 3$ [4] n'a pas de solution (en passant modulo 4, l'équation devient $x^2 + y^2 = 3$ [4] qui n'est jamais vérifiée pour x et y allant de 0 à 3).

première infinité de solutions, la première étant (31, 11), soit n = 15 et m = 11. En composant α' = (11, 4) avec β^k, on trouve une deuxième infinité de solutions, la première solution étant (65, 23), soit n = 32 et m = 23.[29]

Cet exemple est instructif. En effet si l'on veut résoudre $X^2 - dY^2 = K$ ($K \neq \pm 1$), et que l'on connaît une solution particulière α ainsi que la solution primitive β de $X^2 - dY^2 = 1$, on est assuré d'avoir une infinité de solutions de la forme $\alpha\beta^k$, mais on n'est pas assuré de les avoir toutes, comme l'exemple précédent le montre.

Autre remarque : la plus petite solution de $X^2 - 8Y^2 = -7$ est (1, 1) ou $\gamma = 1 + \sqrt{8}$ (elle était sans intérêt dans notre problème). En faisant $\gamma\beta$ on retrouve α = (11, 4). Mais d'où vient α' = (11, 4) ? Il s'agit de $\bar{\gamma}\beta = (1 - \sqrt{8})(3 + \sqrt{8})$.

• *Les maisons d'une rue portent des numéros successifs à partir de 1. Une personne qui habite dans cette rue vous invite chez lui, mais sans donner l'adresse exacte. Il précise seulement que la somme des numéros qui précèdent le numéro de sa propre maison est égale à celle des numéros qui le suivent. Trouver l'adresse sachant que le nombre des numéros de la rue est compris entre 50 et 500.*

Appelons n le nombre de numéros de la rue, et p l'adresse cherchée. On doit avoir :

$1 + 2 + \ldots + (p - 1) = (p + 1) + (p + 2) + \ldots + n$

$$\frac{(p-1)p}{2} = \frac{n(n+1)}{2} - \frac{p(p+1)}{2}$$

$$p^2 - p = n^2 + n - p^2 - p$$

$$2p^2 = n^2 + n$$

$$2p^2 = (n + \frac{1}{2})^2 - \frac{1}{4}$$

$$8p^2 = (2n+1)^2 - 1$$

$$(2n+1)^2 - 8p^2 = 1, \text{ soit } X^2 - 8Y^2 = 1 \text{ avec } X = 2n+1, Y = p$$

La solution primitive est X = 3, Y = 1, mais le résultat pour n et p est sans intérêt.

En composant cette solution avec elle-même, on trouve X = 17, Y = 6, d'où n = 8, p = 6, qui ne convient pas.

La solution suivante est X = 99, Y = 35, d'où n = 49, p = 35 qui ne convient pas.

La suivante est X = 577, Y = 204, soit n = 288, p = 204. L'adresse est au numéro 504.[30]

• *Triangles rectangles presque isocèles à côtés entier : les côtés de l'angle droit mesurent a et a + 1, l'hypoténuse vaut b. Trouver (a, b).*

L'application du théorème de Pythagore conduit à $2a^2 + 2a + 1 = b^2$

$$2(a^2 + a + \frac{1}{2}) = b^2$$

$$2((a + \frac{1}{2})^2 + \frac{1}{4}) = b^2$$

$$\frac{1}{2}((2a+1)^2 + 1) = b^2$$

$$(2a+1)^2 + 1 = 2b^2 \text{ ou } X^2 - 2Y^2 = -1 \text{ avec } X = 2a+1, \; Y = b$$

On a la solution évidente X = 1, Y = 1, d'où a = 0, b = 1 sans intérêt.

En composant (1, 1 ; -1) avec lui-même, on trouve (3, 2 ; 1). Puis en composant (1, 1 ; -1) avec (3, 2 ; 1), on arrive à (7, 5 ; -1) d'où la première solution a = 3, b = 5.

En composant (3, 2 ; 1) avec (7, 5, -1), on a (41, 29, -1) d'où la deuxième solution a = 20, b = 5.

• Trouver *n et p tels que* $C_n^{\,p} = C_{n-1}^{\,p+1}$

$$\frac{n(n-1)\ldots(n-p+1)}{p!} = \frac{(n-1)\ldots(n-p-1)}{(p+1)!}$$

Après simplification $n = \dfrac{(n-p)(n-p-1)}{p+1}$

[29] Ce faisant, on n'a pas pour autant prouvé qu'il n'y a pas d'autres solutions.

[30] Si l'on cherchait la solution suivante, on devrait avoir $X = 8 \times 204 + 3 \times 577$ et n dépasserait largement 500.

$$n^2 - 3np - 2n + p^2 + p = 0$$
$$n^2 - (3p+2)n + p^2 + p = 0$$
$$(n - \frac{3p+2}{2})^2 = \frac{(3p+2)^2}{4} - p^2 - p$$
$$\frac{1}{4}(2n-3p-2)^2 = \frac{5p^2+8p+4}{4}$$
$$(2n-3p-2)^2 = 5(p^2 + \frac{8}{5}p + \frac{4}{5})$$
$$(2n-3p-2)^2 = 5((p+\frac{4}{5})^2 - \frac{16}{25} + \frac{20}{25})$$
$$(2n-3p-2)^2 = \frac{1}{5}((5p+4)^2 + 4)$$
$$(5p+4)^2 - 5(2n-3p-2)^2 = -4$$

C'est de la forme $X^2 - 5\,Y^2 = -4$ avec $X = 5p + 4$ et $Y = 2n - 3p - 2$.
On a le triplet (1, 1 ; -4), qui ne donne rien pour p et n. On trouve aussi (9, 4 ; 1) où (9, 4) est la solution primitive de $X^2 - 5\,Y^2 = 1$.
Par composition, on obtient (29, 13 ; -4), ce qui donne la première solution $p = 5$ et $n = 15$.
Puis composons (9, 4 ; 1) et (29, 13 ; -4), ce qui donne (521, 233 ; -4), mais aucune valeur de p et n ne convient.
Composons encore (9, 4 ; 1) et (521, 233 ; -4), d'où (9349, 4181, ; -4), et la deuxième solution : $p = 1869$ et $n = 4895$.

Bibliographie

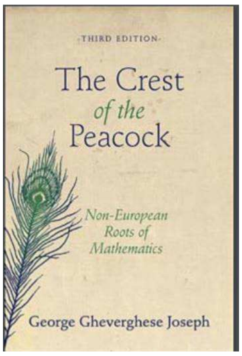
[AYY1930] K. Ayyangar, *New light on Bhaskara's Chakravala or cyclic method of solving indeterminate equations of the second degree in two variables*, in *J. Indian Math. Soc.*, 1929-1930.

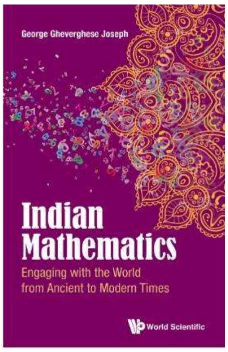
[BAR2003] E. Barbeau, *Pell'Equation*, Springer 2003.

[EDW1977] H.M. Edwards, *Fermat's Last Theorem, a Genetic Introduction to Algebraic Number Theory*, Springer 1977.

[JOS1991] G. Gheverghese Joseph, *The Crest of the Peacock, Non-European Roots of Mathematics*, J.B. Tauris 1991.
Le titre est expliqué par ce poème ancien : « *Comme les crêtes sur les paons, comme les écailles brillantes sur les têtes des serpents, ainsi sont les mathématiques à la tête du savoir* », Vedanga Jyotisa (-500). Le mot *mathématiques* n'existant pas à cette époque, faut il le comprendre comme étant la connaissance des lois du monde ?

[JOS2016] G. Gheverghese Joseph, *Indian Mathematics, Engaging with the World from Ancien to Modern Times*, World Scientific 2016.





[KAT1995] V. J. Katz, *Ideas of Calculus in Islam and India*, Mathematics Magazine, vol. 68, 1995.

[NIV1991] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley 1991.

Annexe 1 : Programme donnant les solutions primitives de l'équation de Pell, et résultats pour *d* de 50 à 209

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
void resultat(double a, double b);
double N(double a, double b);
double d;
double m;

int main()
{ double a,b,c,newa,newb; int i;

for(d=50.;d<100.;d++)
{
 a=1;b=1;
while(N(a,b)<0.)a++;
if (-N(a-1,b)<N(a,b)) a=a-1.;
if (a*a==d) continue;
m=N(a,b);
c=a;
if(fabs(m)==4. || fabs(m)==2. || fabs(m)==1.)
   {resultat(a,b);}
else
{
i=1;
for(;;)
{i++;
c=-c;
while(c<sqrt(d)) c+=fabs(m);
if(d-(c-fabs(m))*(c-fabs(m))<c*c-d)c=c-fabs(m);
newa=(a*c+d*b)/fabs(m);
newb=(a+c*b)/fabs(m);
a=newa;b=newb;
m=N(a,b);
if(fabs(m)==4. || fabs(m)==2 || fabs(m)==1)break;
if (i>50) break;
}
resultat(a,b);
}
}
getchar();return 0;
}

double N(double a, double b)
{return(a*a-d*b*b);
}

void resultat(double a, double b)
{  double X,Y,XX,YY,XXX,YYY;
  printf("\n %3.f : ",d);
  if (fabs(m)==2)
     { X=(a*a+d*b*b)/2.;
      Y=a*b;
      printf(" X=%3.0lf   Y=%3.0lf",X,Y);
     }
  else if (m==-1)
    { X=a*a+d*b*b;
     Y=2.*a*b;
     printf(" X=%3.0lf    Y=%3.0lf",X,Y);
    }
  else if (m==1.)
    {
     X=a; Y=b;
     printf(" X=%3.0lf   Y=%3.0lf",X,Y);
    }
  else if (fabs(m)==4)
    { if ((int)d%4!=0)
       {
        X=(a*a+d*b*b)/2.;Y=a*b;
        XX=(a*X+b*Y*d)/4;YY=(b*X+a*Y)/4;
        if (N(XX,YY)==1)
         printf(" X=%3.0lf    Y=%3.0lf",XX,YY);
        else if (N(XX,YY)==-1)
```

```
            {
             XXX=XX*XX+YY*YY*d; YYY=2.*XX*YY;
             printf(" X=%3.0lf    Y=%3.0lf",XXX,YYY);
            }

          }
        else
          {
           X=(a*a+d*b*b)/4.; Y=a*b/2.;
           printf(" X=%3.0lf   Y=%3.0lf",X,Y);
          }
      }
  }
```

Remarquons que les calculs ne sont pas faits en entiers, mais en *double*, à savoir les nombres (à virgule) les plus grands utilisables par le langage C. Mais ceux-ci peuvent à leur tour être débordés, par exemple pour $d = 2017$, où l'on n'arrive pas au résultat. Pour aller plus loin, il conviendrait d'utiliser l'arithmétique de haute précision. On trouvera ci-dessous des résultats du programme.

```
 50 :  X= 99     Y= 14
 51 :  X= 50    Y=  7
 52 :  X=649    Y= 90
 53 :  X=66249     Y=9100
 54 :  X=485    Y= 66
 55 :  X= 89    Y= 12
 56 :  X= 15    Y=  2
 57 :  X=151    Y= 20
 58 :  X=19603     Y=2574
 59 :  X=530    Y= 69
 60 :  X= 31    Y=  4
 61 :  X=1766319049     Y=226153980
 62 :  X= 63    Y=  8
 63 :  X=  8    Y=  1
 65 :  X=129     Y= 16
 66 :  X= 65    Y=  8
 67 :  X=48842    Y=5967
 68 :  X= 33    Y=  4
 69 :  X=7775     Y=936
 70 :  X=251    Y= 30
 71 :  X=3480    Y=413
 72 :  X= 17    Y=  2
 73 :  X=2281249     Y=267000
 74 :  X=3699     Y=430
 75 :  X= 26    Y=  3
 76 :  X=57799    Y=6630
 77 :  X=351     Y= 40
 78 :  X= 53    Y=  6
 79 :  X= 80    Y=  9
 80 :  X=  9    Y=  1
 82 :  X=163     Y= 18
 83 :  X= 82    Y=  9
 84 :  X= 55    Y=  6
 85 :  X=285769     Y=30996
 86 :  X=10405    Y=1122
 87 :  X= 28    Y=  3
 88 :  X=197    Y= 21
 89 :  X=500001     Y=53000
```

```
 90 :  X= 19    Y=  2
 91 :  X=1574    Y=165
 92 :  X=1151    Y=120
 93 :  X=12151     Y=1260
 94 :  X=2143295    Y=221064
 95 :  X= 39    Y=  4
 96 :  X= 49    Y=  5
 97 :  X=62809633     Y=6377352
 98 :  X= 99    Y= 10
 99 :  X= 10    Y=  1
101 :  X=201     Y= 20
102 :  X=101    Y= 10
103 :  X=227528    Y=22419
104 :  X= 51    Y=  5
105 :  X= 41    Y=  4
106 :  X=32080051     Y=3115890
107 :  X=962    Y= 93
108 :  X=1351    Y=130
109 :  X=158070671986249     Y=15140424455100
110 :  X= 21    Y=  2
111 :  X=295    Y= 28
112 :  X=127    Y= 12
113 :  X=1204353     Y=113296
114 :  X=1025    Y= 96
115 :  X=1126    Y=105
116 :  X=9801    Y=910
117 :  X=649     Y= 60
118 :  X=306917    Y=28254
119 :  X=120    Y= 11
120 :  X= 11    Y=  1
122 :  X=243     Y= 22
123 :  X=122    Y= 11
124 :  X=4620799    Y=414960
125 :  X=930249     Y=83204
126 :  X=449    Y= 40
127 :  X=4730624    Y=419775
128 :  X=577    Y= 51
129 :  X=16855    Y=1484
```

```
130 :  X=6499     Y=570
131 :  X=10610    Y=927
132 :  X= 23   Y=  2
133 :  X=2588599     Y=224460
134 :  X=145925    Y=12606
135 :  X=244   Y= 21
136 :  X= 35   Y=  3
137 :  X=6083073     Y=519712
138 :  X= 47   Y=  4
139 :  X=77563250    Y=6578829
140 :  X= 71   Y=  6
141 :  X= 95   Y=  8
142 :  X=143   Y= 12
143 :  X= 12   Y=  1
145 :  X=289     Y= 24
146 :  X=145   Y= 12
147 :  X= 97   Y=  8
148 :  X= 73   Y=  6
149 :  X=25801741449     Y=2113761020
150 :  X= 49   Y=  4
151 :  X=1728148040    Y=140634693
152 :  X= 37   Y=  3
153 :  X=2177    Y=176
154 :  X=21295    Y=1716
155 :  X=249   Y= 20
156 :  X= 25   Y=  2
157 :  X=46698728731849     Y=3726964292220
158 :  X=7743    Y=616
159 :  X=1324    Y=105
160 :  X=721   Y= 57
161 :  X=11775    Y=928
162 :  X=19601    Y=1540
163 :  X=64080026    Y=5019135
164 :  X=2049    Y=160
165 :  X=1079     Y= 84
166 :  X=1700902565    Y=132015642
167 :  X=168   Y= 13
168 :  X= 13   Y=  1
```

```
170 :  X=339     Y= 26
171 :  X=170   Y= 13
172 :  X=24248647    Y=1848942
173 :  X=2499849     Y=190060
174 :  X=1451    Y=110
175 :  X=2024    Y=153
176 :  X=199   Y= 15
177 :  X=62423    Y=4692
178 :  X=1601    Y=120
179 :  X=4190210    Y=313191
180 :  X=161   Y= 12
181 :  X=2469645423824185900     Y=183567298683461950
182 :  X= 27   Y=  2
183 :  X=487   Y= 36
184 :  X=24335    Y=1794
185 :  X=9249     Y=680
186 :  X=7501    Y=550
187 :  X=1682    Y=123
188 :  X=4607    Y=336
189 :  X= 55   Y=  4
190 :  X=52021    Y=3774
191 :  X=8994000    Y=650783
192 :  X= 97   Y=  7
193 :  X=6224323426849     Y=448036604040
194 :  X=195   Y= 14
195 :  X= 14   Y=  1
197 :  X=393     Y= 28
198 :  X=197   Y= 14
199 :  X=16266196520    Y=1153080099
200 :  X= 99   Y=  7
201 :  X=515095    Y=36332
202 :  X=19731763     Y=1388322
203 :  X= 57   Y=  4
204 :  X=4999    Y=350
205 :  X=39689     Y=2772
206 :  X=59535    Y=4148
207 :  X=1151    Y= 80
208 :  X=649   Y= 45
209 :  X=46551    Y=3220
```

Annexe 2 : Factorisation de Narayana-Fermat

Considérons un nombre N impair. Il peut toujours s'écrire $N = p\,q$ avec $p > q > 0$, qu'il soit premier ou non. Les facteurs p et q sont impairs. Par exemple $15 = 5 \times 3 = 15 \times 1$, et $13 = 13 \times 1$, $9 = 9 \times 1$. On en déduit, puisque $p \pm q$ sont pairs :

$$N = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2 = A^2 - B^2 \text{ avec } A > B > 0 \text{ et } A^2 > N.$$

Tout nombre impair s'écrit comme différence de deux carrés. On peut donc le factoriser : $N = (A + B)(A - B)$. Il reste à déterminer A et B. Pour cela, on essaye les valeurs successives d'un nombre A à partir de la plus petite, jusqu'à ce que l'on tombe sur $A^2 - N$ qui soit un carré, soit B^2.

Supposons en plus que N ne soit pas un carré (sinon la factorisation est déjà faite). Alors $\sqrt{N}$ est un nombre à virgule. Prenons le nombre a égal au nombre entier juste au-desssus de $\sqrt{N}$, soit $a = [\sqrt{N}]+1$. Ce nombre a est le plus petit nombre parmi les nombres A à essayer. Puis formons le nombre positif $r_1 = a^2 - N$. Si l'on tombe sur un carré, soit $b^2 = a^2 - N$, et $N = a^2 - b^2$, c'est fini.

Par exemple, prenons $N = 5523$, $\sqrt{N} = 97{,}...$, d'où $a = 98$. Alors $r = a^2 - N = 81 = 9^2$, d'où $A = 98$ et $B = 9$.
$N = (98 + 9)\,(98 - 9) = 107 \times 89$.

De même avec l'exemple de Narayana : $N = 1161$. On trouve $a = 35$ et $r = 35^2 - N = 64 = 8^2$, d'où
$N = 35^2 - 8^2 = (35 + 8)(35 - 8) = 43 \times 27$. [31]

Mais le nombre r_1 n'est pas toujours un carré, loin s'en faut. Alors on recommence avec le nombre $a + 1$ en prenant $r_2 = (a + 1)^2 - N$. Si c'est un carré, c'est gagné, sinon on recommence avec $r_3 = (a + 2)^2 - N$, et ainsi de suite tant qu'on l'on n'a pas un carré. On est sûr que le procédé finit par s'arrêter, puisque N s'écrit toujours $A^2 - B^2$.

Par exemple, pour $N = 7169$, on a :
$a = 85$ $\quad r_1 = 56$
$a + 1 = 86$ $\quad r_2 = 227$
$a + 2 = 87$ $\quad r_3 = 400 = 20^2$, d'où $7169 = 87^2 - 20^2 = 107 \times 67$.

---

[31] En fait, Narayana ne prend pas le plus petit entier a au-dessus de $\sqrt{N}$, mais le plus grand entier a_0 au-dessous, d'où $a_0 = 34$ et $a_0^2 - N = -5$. On en déduit que $(a_0 + 1)^2 - N = -5 + 2a_0 + 1 = 64 = 8^2$, et la factorisation $(a_0 + 1 + b)(a_0 + 1 - b) = (35 + 8)(35 - 8)$.

On vérifie facilement que de r_1 à r_2 l'augmentation est de $u_0 = 2a + 1$, que de r_2 à r_3 l'augmentation est de $2a + 3 = u_0 + 2$, que de r_3 à r_4 l'augmentation est de $2a + 5 = u_0 + 4$, et ainsi de suite. En appelant $m + 2$ le nombre total des étapes de calcul, jusqu'à l'obtention d'un carré, on a

$r_{m+2} = r_1 + u_0 + (u_0 + 2) + (u_0 + 4) + ... + (u_0 + 2m) = b^2$ et aussi $r_{m+2} = (a + m + 1)^2 - N$, d'où
$N = (a + m + 1)^2 - b^2$

Reprenons l'exemple attribué (peut-être) à Narayana : $N = 1001$. On commence par $a = 32$ et $r_1 = 23$.[32] Et avec $u_0 = 2a + 1 = 65$, on arrive à $r_{14} = 23 + 65 + 67 + 69 + 71 + ... + 89 = 1024 = 32^2$. C'est bien ce que donne le programme :

```
N = 1001
a= 32   r=  23
a= 33   r=  88
a= 34   r= 155
a= 35   r= 224
a= 36   r= 295
a= 37   r= 368
a= 38   r= 443
a= 39   r= 520
a= 40   r= 599
a= 41   r= 680
a= 42   r= 763
a= 43   r= 848
a= 44   r= 935
a= 45   r= 1024    b= 32

1001 =   77  x  13      nombre de pas = 14
```

Le programme découle de ce qui précède.

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
double N;

int main()
{ double a,r,b,bb,u0,F1,F2; int m,nbpas;
  N=100895598169.;
  a=(int)(sqrt(N)+1); r=a*a-N;   printf("\n  N = %3.lf   \n  a=%3.lf  r=%3.lf",N, a,r);  /* calcul de a et r = a2 – N */
   b=sqrt(r);  bb=(int)b;
   if (bb*bb==r)              /* cas particulier où l'on tombe aussitôt sur un carré */
       {printf(" *** b= %3.0f",b);
        F1=a+b; F2=a-b;
        printf("\n\n    %3.lf = %3.f  x %3.f",N,F1,F2);
       }
   else
     { m=0; u0=2*a+1; nbpas = 1;
       for(;;)
         {  nbpas++;
            r+=u0+2*m;  /* évolution de r à chaque étape */
            b=sqrt(r);
            printf(" \n  a=%3.f  r= %3.f",a+m+1,r);     /* affichage à supprimer pour N grand */
            bb=(int)b;
            if (bb*bb==r)   /* cas où l'on tombe finalement sur un carré */
               { printf("  a= %3.f  b=%3.0f",a+m+1,b);
                 F1=m+a+1+b; F2=m+a+1-b;
                 printf("\n\n  %3.lf = %3.lf  x %3.lf",N,F1,F2);
                 printf("     nombre de pas = %d",nbpas);
                 break;
               }
            m++;   /* m augmente de 1 à chaque étape */
          }
     }
  getchar();return 0;
}
```

Reprenons les exemples traités par Fermat :

- $N = 10\,235\,789$. Nous avons affiché ci-dessous la première valeur de a et la dernière, avec la factorisation finale au bout de 26 étapes de calcul, telle qu'elle est donnée par le programme :

```
N = 10235789
a=3200   r= 4211

a= 3225    b=406

10235789 = 3631   x 2819      nombre de pas = 26
```

[32] On peut aussi bien commencer par $a_0 = 31$ et $r_0 = -40$, ce qui donne à l'étape suivante $a_1 = 32$ et $r_1 = -40 + 63 = 23$.

- N = 100 895 598 169. Il y a 187 723 étapes de calcul pour arriver au résultat :

```
N = 100895598169
a=317641  r= 206712

a= 505363   b=393060

100895598169 = 898423  x 112303      nombre de pas = 187723
```

Au cas, même très improblable, où Fermat se serait inspiré de méthodes indiennes, il n'en reste pas moins que les dimensions des nombres qu'il a factorisés sont sans commune mesure avec les exemples venus d'Inde. Au point que les raccourcis de calcul qu'il a dû trouver restent encore mystérieux de nos jours (on pourra consulter à ce sujet *Savez-vous factoriser à la mode de Fermat ? Blogdemaths, 2014*, où trois hypothèses sont évoquées)..