*Le mot* algorithme *provient de la version latinisée du nom du mathématicien persan Al-Khwarizmi[1]. Cependant, les mathématiciens avaient développé et mis en œuvre des algorithmes bien avant sa naissance.*

*Al-Khwarizmi*
*783-850*

# Algorithmes
## au cours de l'histoire

**André Ross**
Professeur retraité

Dans l'article *Extraction d'une racine dans un carré*[2], Bernard Hodgson nous a déjà présenté un algorithme connu mille ans avant Pythagore et utilisé par les Mésopotamiens de l'Antiquité pour extraire une racine carrée. En fait, dès que l'on cherche à résoudre systématiquement une famille de problèmes, on est déjà à la recherche d'un algorithme.

### Algorithme d'Euclide

Un algorithme que le lecteur a probablement déjà utilisé est appelé l'*algorithme d'Euclide*. On le retrouve dans le Livre VII des *Éléments* d'Euclide, qui vécut à Alexandrie environ un millénaire avant Al-Khwarizmi. Cet algorithme permet de trouver le plus grand commun diviseur, ou pgcd, de deux nombres.

Dans la tradition euclidienne, un nombre entier est une longueur et un produit d'entiers est un rectangle, comme l'indique la définition suivante tirée de la traduction de Bernard Vitrac des *Éléments* d'Euclide :

*Et quand deux nombres, s'étant multipliés l'un l'autre, produisent un certain nombre, le produit est appelé* plan, *et les nombres qui se sont multipliés l'un l'autre, ses* côtés.

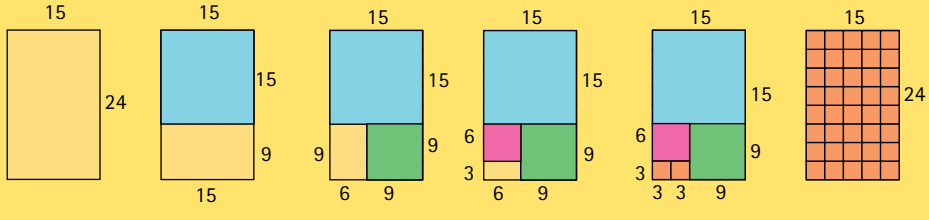
(Livres VII, définition 17,)

La procédure pour déterminer le pgcd de deux nombres, telle qu'illustrée ci-dessous, consiste d'un point de vue géométrique à déterminer la longueur du côté du plus grand carré à l'aide duquel on peut paver entièrement le rectangle dont les longueurs des côtés sont les nombres dont on cherche le pgcd.

En procédant numériquement, par divisions successives de la longueur par la largeur, puis de la largeur par le reste, et ainsi de suite jusqu'à un reste nul, on obtient

$$24 = 1 \times 15 + 9$$
$$15 = 1 \times 9 + 6$$
$$9 = 1 \times 6 + 3$$
$$6 = 2 \times 3 + 0$$

Le pgcd étant le dernier reste non nul de ce processus, 3 est donc le plus grand commun diviseur de 24 et 15. On écrit pgcd(15, 24) = 3.




Dans le rectangle de côtés 24 et 15, on peut inscrire un carré de côté 15. Il reste un rectangle de côtés 9 et 15 dans lequel on peut inscrire un carré de côté 9. Il reste un rectangle de côtés 9 et 6, à l'intérieur duquel on peut inscrire un carré de côté 6, il reste un rectangle de cotés 6 et 3 dans lequel on inscrit maintenant deux carrés de côté 3. C'est le plus grand carré à l'aide duquel on peut paver le rectangle initial. 3 est donc le pgcd de 24 et 15. Lorsque le plus grand carré permettant de paver le rectangle est unitaire, les nombres *sont premiers entre eux.*

1. *Le mot algèbre vient de* Al-jabr wa'l muqabala, *titre d'un livre d'Al-Khwarizmi. Cet ouvrage est le texte fondateur de l'algèbre.*
2. *Voir* Accromath, *volume 1, automne-été 2006.*

Il est à noter qu'en utilisant l'algorithme d'Euclide, on peut déterminer le pgcd de deux nombres sans connaître leur factorisation en nombres premiers. La factorisation des nombres 15 et 24 est simple à obtenir,

$$15 = 3 \times 5 \text{ et } 24 = 3 \times 2^3,$$

d'où on peut conclure immédiatement que pgcd(15, 24) = 3. Cependant, pour de très grands nombres, il est plus simple et nettement plus rapide d'appliquer l'algorithme d'Euclide, même à l'aide d'un ordinateur.

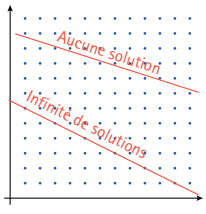
## Algorithme d'Euclide et équations diophantiennes

Rappelons qu'une *équation diophantienne* est une équation polynomiale à une ou plusieurs inconnues dont les solutions sont cherchées parmi les nombres entiers, les coefficients étant eux-mêmes des entiers. On a recours à l'algorithme d'Euclide pour résoudre certaines équations diophantiennes de la forme

$$ax + by = c.$$

À quelles conditions une telle équation admet-elle une solution entière ?

En ayant recours à la géométrie analytique moderne, on peut visualiser le problème comme suit. L'ensemble des solutions de l'équation $ax + by = c$ est représenté par une droite. Si aucun point de la droite n'a de coordonnées entières, l'équation n'a aucune solution.




Mais, si la droite passe par au moins un point de coordonnées entières, elle a alors une infinité de solutions puisque $a$, $b$ et $c$ sont des entiers.

Deux théorèmes apportent des réponses pour certaines de ces équations.

## Théorème de Bachet-Bézout

*Soit a et b deux entiers. Si d est le pgcd de a et b, alors il existe des entiers x et y tels que*

$$ax + by = d = \text{pgcd}(a, b).$$

Le second théorème porte sur le cas où les deux entiers $a$ et $b$ ont 1 comme seul facteur commun.

### Diophante d'Alexandrie

On ignore tout de la vie du mathématicien grec Diophante, dont on ne connaît que les écrits. On pense qu'il vivait vers le 3e siècle de notre ère, sans pouvoir apporter plus de précisions. Son ouvrage le plus célèbre est un traité de 13 livres, les *Arithmétiques*. Six volumes de cet ouvrage, rédigés en grec, ont été retrouvés en Italie au 15e siècle par Regiomontanus (Johann Müller (1436-1476)). Quatre autres livres, traduits en arabe, ont été découverts en Iran en 1968. Les experts ne s'entendent pas à leur sujet : s'agit-il de la traduction du texte original de Diophante, ou plutôt d'un commentaire sur les *Arithmétiques*, peut-être écrit par Hypathie (env. 355-415)?

Les *Arithmétiques* sont une collection de 189 problèmes accompagnés de leur solution conduisant à des équations dont les solutions sont entières ou fractionnaires.

### Claude-Gaspard Bachet de Méziriac (1581-1638)

Claude-Gaspard Bachet de Méziriac est un mathématicien, poète et traducteur français. Le théorème qui porte son nom a été présenté pour la première fois dans la deuxième édition de son ouvrage « *Problèmes plaisans et délectables qui se font par les nombres* », parue en 1624.

## Théorème de Bézout

*Deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers x et y tels que*

$$ax + by = 1.$$

À propos de ces théorèmes, si la constante, $d$ ou 1 selon le cas, n'est pas le pgcd des coefficients, on ne peut rien conclure. Par ailleurs, pour déterminer une première solution $(x_0; y_0)$ d'une équation de la forme

$$ax + by = \text{pgcd}(a, b),$$

on utilise l'algorithme d'Euclide et à l'aide du *lemme de Gauss*, on généralise celle-ci en montrant que

$$a\left(x_0 - k\frac{b}{d}\right) + b\left(y_0 + k\frac{a}{d}\right) = d,$$

où $k$ est un nombre entier.

### Lemme d'Euclide

*Si un nombre premier* p *divise le produit de deux nombres entiers* b *et* c, *alors* p *divise* b *ou* c.

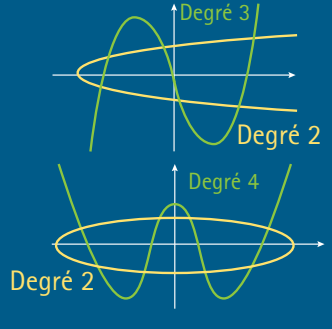
(Éléments, *proposition VII.30)*

### Lemme de Gauss

*Si un nombre entier* a *divise le produit de deux autres nombres entiers* b *et* c, *et si* a *est premier avec* b, *alors* a *divise* c.

### Étienne Bézout (1730-1783)

Le mathématicien français Étienne Bézout est passé à la postérité pour le théorème de Bachet-Bézout en arithmétique. Il est le premier à donner une démonstration correcte du théorème suivant selon lequel deux courbes algébriques, respectivement de degré $m$ et $n$, se rencontrent en général en $mn$ points, en comptant les multiplicités.



## Résolution à l'aide de l'algorithme d'Euclide

Considérons l'équation

$$510x + 294y = 6.$$

Cette équation admet-elle des solutions ? En appliquant l'algorithme d'Euclide, on obtient que :

$$\left.\begin{array}{l} 510 = 1\times294 + 216 \\ 294 = 1\times216 + 78 \\ 216 = 2\times78 + 60 \\ 78 = 1\times60 + 18 \\ 60 = 3\times18 + 6 \\ 18 = 3\times6 + 0 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} 216 = 510 - 1\times294 \\ 78 = 294 - 1\times216 \\ 60 = 216 - 2\times78 \\ 18 = 78 - 1\times60 \\ 6 = 60 - 3\times18 \end{array}\right.$$

On isole les restes

Dans la colonne de gauche, le dernier reste non nul est 6, on a donc pgcd(294, 510) = 6. Par conséquent, le théorème de Bachet-Bézout nous garantit que l'équation admet une solution $(x_0; y_0)$. On détermine celle-ci en isolant les restes, ce qui est fait dans la colonne de droite. On substitue ensuite en « remontant la chaîne » de calculs afin d'exprimer 6 en termes de 294 et de 510.

Cela donne :

$$6 = 60 - 3\times\overbrace{(78 - 1\times60)}^{18} = 4\times60 - 3\times78$$

$$6 = 4\times\overbrace{(216 - 2\times78)}^{60} - 3\times78 = 4\times216 - 11\times78$$

$$6 = 4\times216 - 11\times\overbrace{(294 - 1\times216)}^{78} = 15\times216 - 11\times294$$

$$6 = 15\times\overbrace{(510 - 1\times294)}^{216} - 11\times294 = 15\times510 - 26\times294$$

Par conséquent, le couple (15; −26) est une solution de l'équation $510x + 294y = 6$. L'ensemble des solutions entières est formé de tous les couples de la forme $(15 - 49k; -26 + 85k)$, où $k$ est un entier.

| | |
|---|---|
| 1 | 23 |
| 2 | 46 |
| 4 | 92 |
| 8 | 184 |
| 16 | 368 |
| 32 | |

| | |
|---|---|
| 1 | 23 |
| 2 | 46 |
| ~~4~~ | ~~92~~ |
| ~~8~~ | ~~184~~ |
| 16 | 368 |
| 19 | 437 |

NUMÉRATION HIÉROGLYPHIQUE
Valeur des symboles

- Le bâton représente l'unité.
- L'anse de panier, la dizaine.
- Le rouleau de papyrus, la centaine.
- La fleur de lotus, le millier.
- Le doigt désignant les étoiles, dix mille.
- Le têtard, cent mille.
- Le dieu agenouillé soutenant le monde, un million.

## Multiplication égyptienne

Dans tous les systèmes de numération, on a eu recours à des algorithmes pour effectuer des opérations.

Ainsi, pour multiplier 19 par 23, le scribe égyptien associe le plus grand des deux nombres à l'unité et double ces nombres[4]. Il arrête lorsque le nombre de la colonne de gauche devient plus grand que le multiplicateur.

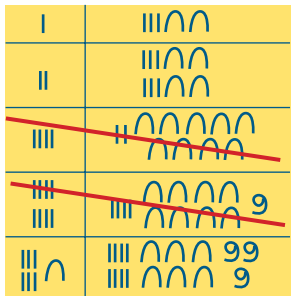
Puisque 19 = 16 + 2 + 1, il additionne les nombres de la colonne de droite sur les lignes non biffées, ce qui donne :

$$19\times23 = 23 + 46 + 368 = 437.$$

On qualifie le système de numération égyptien de système additif de base dix. Il est additif car c'est par la répétition des symboles que l'on écrit un nombre, et de base dix, car un nouveau symbole est utilisé pour chaque puissance de dix.

*4. Il est intéressant de noter que la méthode égyptienne peut être vue en termes modernes comme revenant à écrire le multiplicateur en base deux (même si leur système de numération n'était pas un système positionnel comme le nôtre).*

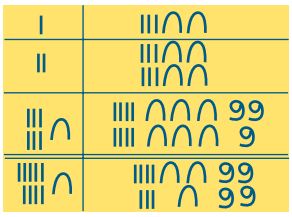
Dans ce système, pour multiplier un nombre par 2, il suffit de doubler le nombre de symboles et d'effectuer les regroupements en remplaçant tout groupe de 10 symboles identiques par le symbole supérieur. En utilisant cette écriture des nombres, la multiplication que nous venons d'effectuer s'écrit de la façon ci-bas.



On arrête lorsqu'en doublant dans la colonne de gauche, on obtient un nombre plus grand que le multiplicateur (en doublant les symboles du dernier nombre de la colonne de gauche, on obtiendrait deux symboles ∩ suivis de plusieurs symboles I, ce qui est plus grand que le multiplicateur).

Le scribe repère alors dans la colonne de gauche les nombres qui additionnés donnent le multiplicateur, soit

Il suffit d'additionner les résultats des lignes dont la somme donne le multiplicateur, ce qui donne :



En écriture moderne, le scribe exprime le multiplicateur comme somme de puissances de 2, soit :

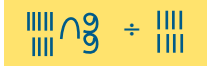
$$19 = 16 + 2 + 1.$$

En doublant la valeur du multiplicande et en retenant, les valeurs correspondant aux termes de la décomposition du multiplicateur en somme de puissances de 2, il obtient :

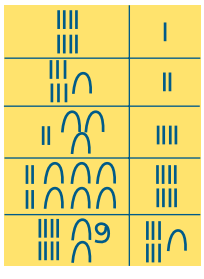
$$\begin{aligned} 23\times19 &= 23\times(16 + 2 + 1) \\ &= 368 + 46 + 23 \\ &= 437. \end{aligned}$$

## Division égyptienne

Pour illustrer comment s'effectue une division, considérons l'opération



Le scribe associe le diviseur à l'unité et il double successivement jusqu'à obtenir le plus grand multiple du diviseur inférieur au nombre à diviser.



Dans ce tableau, le scribe détecte aisément qu'en doublant le nombre de la colonne de gauche il obtiendrait un nombre plus grand que le dividende. En effet, il obtiendrait alors deux symboles 9 suivis de deux symboles ∩ (lecture de droite à gauche) alors que le dividende est formé de deux symboles 9 suivi d'un seul symbole ∩.

Le dividende peut alors s'exprimer comme la somme de certains des nombres de la colonne de gauche plus possiblement un reste plus petit que le diviseur.

Le scribe fait la somme des nombres des deux dernières lignes de la colonne de gauche, ce qui donne un nombre plus petit que le dividende. En effet, elle ne contient qu'un seul symbole 9 alors que le dividende en a deux. (En langage moderne, le chiffre des centaines est trop petit.)

De plus, il peut facilement constater qu'en additionnant à ce résultat le nombre de la troisième ligne à partir du bas, il va obtenir deux symboles 9 suivis de deux symboles ∩. La somme serait donc plus grande que le dividende qui est formé de deux symboles 9 suivi d'un seul symbole ∩. Cette somme serait plus grande que le dividende, ce qui signifie que le nombre de la troisième ligne à partir du bas ne fait pas partie du développement du dividende en somme de multiples du diviseur. Il faut biffer cette ligne dans le tableau.

En ajoutant plutôt le nombre de la quatrième ligne à partir du bas et en comparant le résultat au dividende, il constate que cette somme est plus petite que le dividende (elle ne contient pas le symbole ∩ alors que le dividende en a un et le diviseur est plus petit que ∩.)

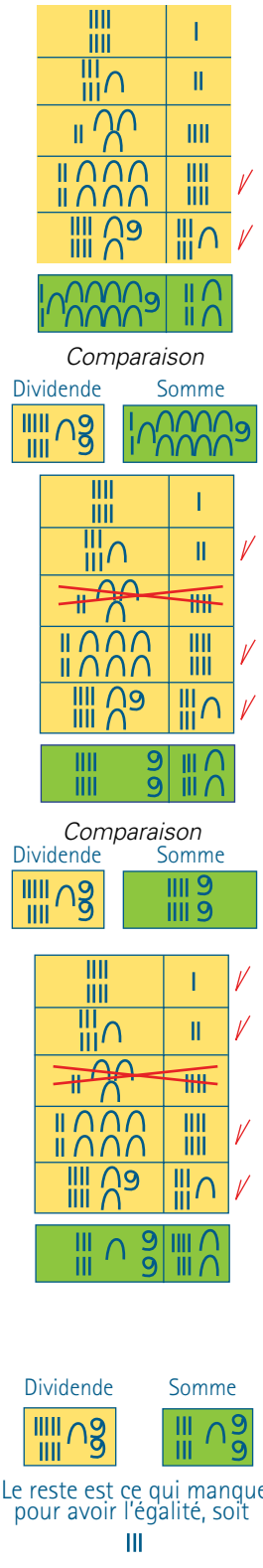
Il ajoute alors le nombre de la ligne du haut. En comparant le dividende et la somme obtenue, le scribe peut facilement constater que le reste est 3.

En effectuant la somme des nombres conservés dans la colonne de droite, le scribe détermine le quotient. Il a donc obtenu :

$$219 = 27 \times 8 + 3.$$

De nos jours, on écrirait le quotient

$$27\frac{3}{8} \text{ ou } 27{,}375.$$



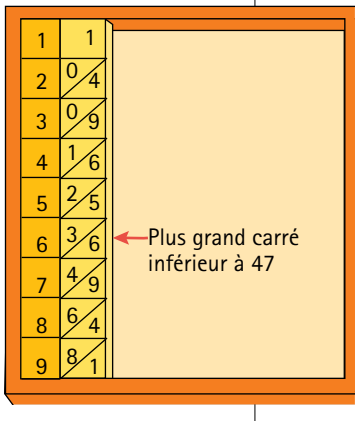
*Le symbole ∧ désigne une addition alors que ∧ indique une soustraction.*

Pour représenter une fraction, le scribe égyptien inscrivait l'hiéroglyphe ⬭ au-dessus d'un nombre. Ainsi, pour représenter la fraction 1/12, le scribe doit écrire 𓂝𓎆. Cette façon de faire a un inconvénient : le numérateur des fractions est toujours l'unité (sauf pour 2/3, pour lequel on disposait d'un hiéroglyphe particulier).

Pour indiquer 3/8, le scribe devait donc considérer que 3/8 = 1/4 + 1/8 et écrire :

## Réglettes de Napier et extraction de racines

La multiplication et la division en numération égyptienne illustrent le fait qu'un algorithme dépend du système de numération utilisé. Il peut aussi dépendre de l'instrument de calcul utilisé. Napier a développé un algorithme pour extraire une racine carrée à l'aide de ses réglettes[5].




L'algorithme de Napier repose sur la méthode traditionnelle « à la main » pour extraire une racine carrée[6]. Il considère une réglette supplémentaire (en jaune dans les illustrations) représentant les carrés des nombres de 1 à 9. L'algorithme s'applique à un nombre s'écrivant avec un nombre pair de chiffres, que l'on divise en tranches de deux chiffres (si ce n'est pas le cas, on ajoute un 0 à la gauche du nombre). Effectuons l'extraction de la racine carrée du nombre 463 856.

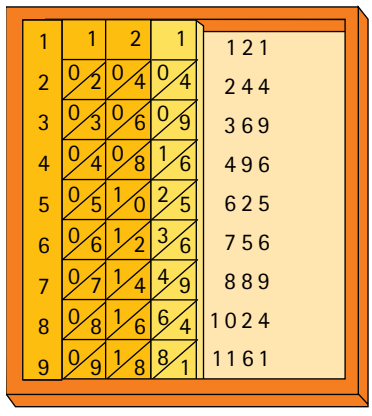
Dans ce nombre, la première tranche de deux chiffres est 46. Le plus grand chiffre dont le carré est inférieur à 46 est 6. C'est le premier chiffre du résultat :

$$\sqrt{463\,856} = 6....$$

En soustrayant de 46 le carré de 6, on obtient 10 et on abaisse les deux chiffres suivant du nombre à extraire.

$$\begin{array}{r} 463\,856 \\ -36 \\ \hline 1038 \end{array}$$

On dispose dans le plateau les réglettes du double du premier chiffre du résultat (ici les réglettes 1 et 2 pour 12) suivies de la réglette




jaune et on repère le nombre qui précède immédiatement 1 038 dans ceux représentés par les lignes du plateau. Sur la huitième ligne, on lit 1 024,

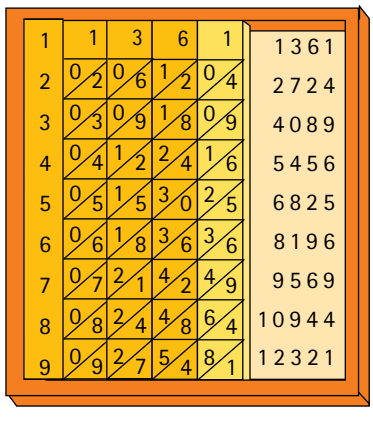
Le deuxième chiffre de la racine carrée est donc 8.

$$\sqrt{463\,856} = 68....$$

On soustrait 1 024 de 1 038, ce qui donne 14 et on abaisse la tranche des deux chiffres suivants du nombre à extraire, ce qui donne 1 456.

On double le second chiffre de la racine, $2 \times 8 = 16$ que l'on ajoute au nombre 12 déjà formé en le multipliant par 10, soit $12 \times 10 + 16 = 136$.

On dispose dans le plateau les réglettes du nombre 136, suivis de la réglette jaune et on



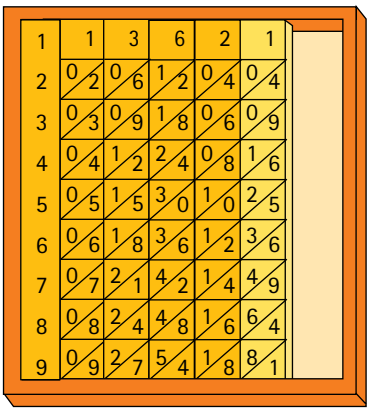

5. *Les algorithmes pour la multiplication et la division à l'aide de réglettes ont été présentés dans l'article «John Napier»,* Accromath, *Vol. 14, hiver-printemps 2019.*
6. *L'algorithme traditionnel pour la racine carrée fait l'objet du problème « Racines cristallines » d'*Accromath *(vol. 11, été-automne 2016, p. 32), en lien avec le texte « Glanures mathématico-littéraires (II) » de Bernard R. Hodgson.*

repère le nombre qui précède immédiatement 1 456. Sur la première ligne, on a 1 361. Le troisième chiffre de la racine est donc 1,

$$\sqrt{463\,856} = 681....$$

En soustrayant, 1 361 de 1 456, on obtient 95. C'est la dernière tranche de deux chiffres du nombre dont on veut extraire la racine, on ajoute une virgule décimale et on abaisse 00 pour obtenir 9 500.

On double le troisième chiffre de la racine, $2\times 1=2$ que l'on ajoute au nombre déjà formé que l'on multiplie par 10, soit $136\times 10+2=1\,362$. On dispose dans le plateau les réglettes du nombre 1 362, suivis de la réglette jaune. On remarque que le nombre sur la ligne 1 est plus grand que 9500. On ajoute un 0 après la virgule décimale,



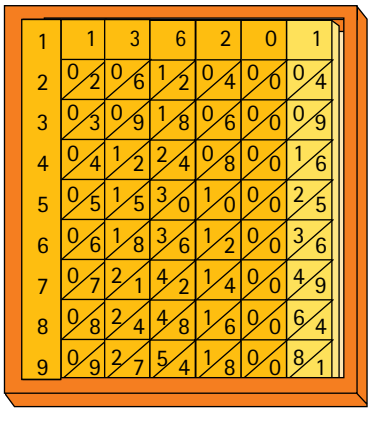

$$\sqrt{463\,856} = 681{,}0....$$

et on abaisse à nouveau 00, ce qui donne 950 000. On intercale la réglette de 0 avant la réglette jaune.

On repère le nombre qui précède immédiatement 950 000, c'est 817 236 sur la ligne 6. Le deuxième chiffre après la virgule décimale est donc 6. Ce qui donne

$$\sqrt{463\,856} = 681{,}06....$$

On poursuit ainsi en abaissant 00 à chaque étape jusqu'à ce que l'on obtienne la précision cherchée.




136 201
272 404
408 609
544 816
681 025
817 236
953 449
1 089 664
1 225 881

## Pour y voir plus clair

On cherche à exprimer le nombre dont on veut extraire la racine carrée sous la forme

$$463\,856 = (a\times 10^2 + b\times 10 + c)^2 + R,$$

car il est clair que la partie entière de cette racine carrée s'écrit avec trois chiffres.

À chaque étape du calcul, on exprime le nombre comme somme d'un carré parfait et d'un terme résiduel, allant chercher un des trois chiffres $a$, $b$ et $c$ à la fois.

À la première étape, on a donc

$$\begin{aligned} 463\,856 &= 6^2\times 100^2 + 103\,856 \\ &= (6\times 10^2)^2 + 103\,856. \end{aligned}$$

À l'issue de la seconde étape, on obtient

$$\begin{aligned} 463\,856 &= 6^2\times 100^2 + 103\,856 \\ &= (6\times 10^2 + 8\times 10)^2 + 1\,456. \end{aligned}$$

Et à l'issue de la troisième étape, on obtient enfin

$$\begin{aligned} 463\,856 &= 6^2\times 100^2 + 103\,856 \\ &= (6\times 10^2 + 8\times 10 + 1)^2 + 95. \end{aligned}$$

La partie entière de la racine carrée de 463 856 est donc 681. Pour trouver la partie décimale de cette racine, il s'agit maintenant de poursuivre les calculs sur la partie résiduelle $R = 95$.

## Conclusion

Le vocable *algorithme* est devenu d'usage courant avec l'avènement des ordinateurs. Cependant, des algorithmes ont été développés très tôt dans l'histoire. Dès que les premiers systèmes de numération sont apparus, on a développé des algorithmes pour effectuer les opérations usuelles : addition, soustraction, multiplication, division. En cherchant à résoudre des problèmes plus élaborés comme l'extraction de racines ou la recherche du pgcd de deux nombres entiers, il a fallu développer d'autres algorithmes, plus poussés et parfois étonnants.