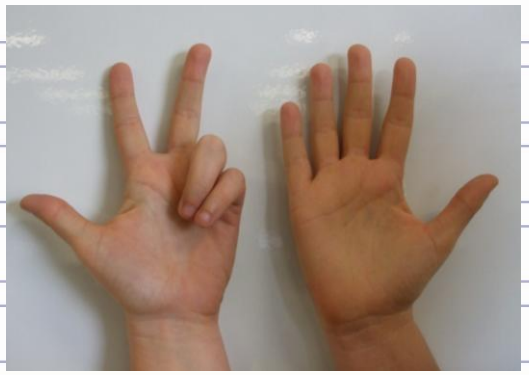
N° 125 – Novembre 2012

Feuille de Vigne

Irem de Dijon

- ✓ Géométrie sur une image
- ✓ Multiplications : Techniques avec les doigts
- ✓ Comment fabriquer de grands nombres premiers ?



Revue Trimestrielle

Issn 0246-5752

Sommaire

Articles

Éditorial

Qu'avons-nous dans ce numéro 125 ?

D'abord, Alain Mascret, dans le numéro 124, nous avait montré comment insérer une image dans une figure issue d'un logiciel de géométrie dynamique tel geogebra. Cela nous avait permis de constater que dans "Le couronnement de la vierge" de Zanobi di Machiavelli, les auréoles des angelots sont des ellipses.
Il récidive dans ce numéro, non pas pour déterminer le sexe des anges du tableau, (ce sera peut-être pour le numéro 126) mais pour l'étude des transformations géométriques qui se fait d'une manière beaucoup plus agréable avec des images de bâtiments ou des photographies qu'avec de bêtes carrés.

Marie Noëlle Racine, prévoyant que dans un futur proche nous oublierons plus ou moins vite nos tables de multiplication, nous rappelle de vieilles recettes utilisant les doigts des deux mains, recettes dues à Antoine ARNAULD janséniste du XVII^{e}.

Michel Lafond est parti à la chasse des très grands nombres premiers armé d'une simple calculette, voire d'une simple feuille de papier et d'un crayon. Il ressort pour l'occasion un théorème (datant de 1916) d'un obscur prof de maths dénommé Pocklington. Là aussi, bien que ce ne soit pas évident, il y a des applications concrètes.

Michel Lafond

Jeux et Problèmes

Michel LAFOND
mlafond001@yahoo.fr

JEU – 75.

Démontrer sans calculette que :

$$\frac{(9994^4+4)(9998^4+4)}{(9995^4+4)(9996^4+4)} = \frac{(9993^2+1)(9999^2+1)}{(9994^2+1)(9996^2+1)}$$

PROBLÈME – 75.

Pour résoudre l'équation (1) $e^{x-2} + e^{x+8} = e^{4-x} + e^{3x+2}$ un élève dit :

On sait que $e^a + e^b = e^{a \times b}$ et que l'exponentielle est bijective.
Donc (1) $\Leftrightarrow$ $(x-2)(x+8) = (4-x)(3x+2)$
Je développe : $x^2 + 6x - 16 = -3x^2 + 10x + 8$
Je réduis : $4x^2 - 4x - 24 = 0$
Je factorise : $4(x+2)(x-3) = 0$
Les solutions sont $x = -2$ ou $x = 3$.

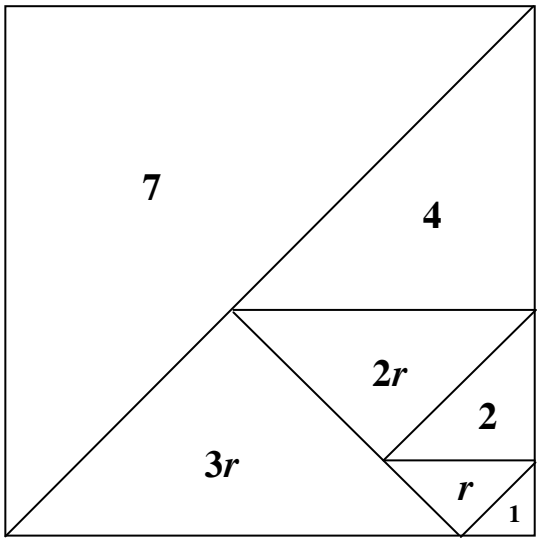
Quelle note lui mettez-vous ?

Solutions

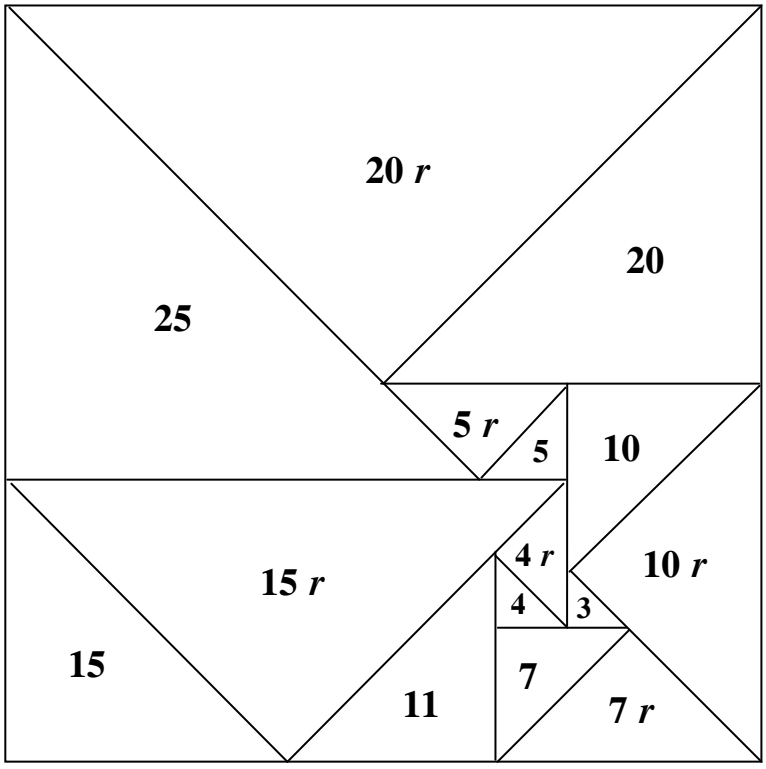
JEU – 74.
Il est assez facile de partager un carré en un nombre fini de triangles rectangles isocèles tous inégaux en tailles.
Il est plus difficile de partager un carré en un nombre fini de triangles rectangles isocèles tous inégaux en tailles si on interdit le tracé d'une diagonale du carré.
Saurez-vous résoudre ces deux énigmes ?

Solution :

Si on a droit à la diagonale, on a par exemple la solution ci-dessous dans laquelle on a posé $r = \sqrt{2}$. Le nombre inscrit dans un triangle est son côté.



Si on n'a pas droit à la diagonale, on a la solution ci-dessous qui n'est peut-être pas la plus simple :



PROBLÈME – 74.

Quelle est la particularité de la courbe de représentation paramétrique :

$$x(t) = 10\cos^{6}(t) - 15\cos^{8}(t) + 6\cos^{10}(t)$$
$$y(t) = 10\sin^{6}(t) - 15\sin^{8}(t) + 6\sin^{10}(t)$$

si $t \in [0\ ,\ \pi/2]$?

Solution :

Cette courbe est un segment de droite ! (qu'on peut admirer en bas) En effet :

Posons $u_n = \cos^{2n}(t) + \sin^{2n}(t)$ $\quad c = \cos(t)$ et $s = \sin(t)$.

On a : $u_0 = 2$ $\quad u_1 = 1$ $\quad u_2 = c^4 + s^4 = (c^2 + s^2)^2 - 2\,c^2\,s^2 = 1 - 2\,c^2\,s^2$.

Puis :

$$\begin{aligned} u_{n+1} - c^2\,s^2\,u_n &= \cos^{2n+2}(t) + \sin^{2n+2}(t) - c^2\,s^2\,(\cos^{2n}(t) + \sin^{2n}(t)) \\ &= \cos^{2n+2}(t) + \sin^{2n+2}(t) - \cos^{2n+2}(t)\,(1 - c^2) - \sin^{2n+2}(t)\,(1 - s^2) \\ &= \cos^{2n+4}(t) + \sin^{2n+4}(t) = u_{n+2} \end{aligned}$$

Donc, si on pose $p = c^2\,s^2$ on a la récurrence $u_{n+2} = u_{n+1} - p\,u_n$

On en tire :

$u_2 = c^4 + s^4 = 1 - 2\,p$. [déjà vu plus haut]

$u_3 = c^6 + s^6 = u_2 - p\,u_1 = 1 - 3\,p$.

$u_4 = c^8 + s^8 = u_3 - p\,u_2 = 1 - 3\,p - p\,(1 - 2\,p) = 1 - 4\,p + 2\,p^2$.

$u_5 = c^{10} + s^{10} = u_4 - p\,u_3 = 1 - 4\,p + 2\,p^2 - p\,(1 - 3\,p) = 1 - 5\,p + 5\,p^2$.

Donc $10\,u_3 - 15\,u_4 + 6\,u_5 = 10\,(1 - 3\,p) - 15\,(1 - 4\,p + 2\,p^2) + 6\,(1 - 5\,p + 5\,p^2) = 1$.

Autrement dit : $x(t) + y(t) = 1$.

Cela prouve que la courbe est incluse dans la droite $X + Y = 1$.

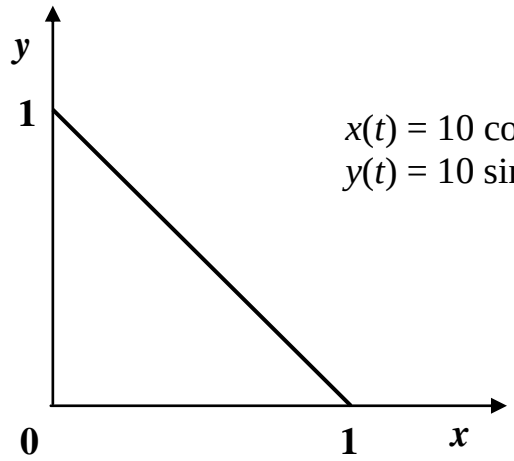
Pour déterminer la partie de cette droite concernée, remarquons que :

$x(t) = \varphi(c) = 6\,c^{10} - 15\,c^8 + 10\,c^6$ où $c = \cos(t)$ décrit $[0 ; 1]$.

Or $\varphi'(c) = 60\,c^5\,(c^4 - 2\,c^2 + 1) = 60\,c^5\,(c^2 - 1)^2$ est positive donc φ est croissante.

Enfin, $x(0) = \varphi(1) = 1$ et $x(\pi/2) = \varphi(0) = 0$ prouve que x décrit $[0 ; 1]$

La courbe est le segment en gras ci-dessous.



$$x(t) = 10\cos^6(t) - 15\cos^8(t) + 6\cos^{10}(t)$$
$$y(t) = 10\sin^6(t) - 15\sin^8(t) + 6\sin^{10}(t)$$

$$t \in [0\ ,\ \pi/2]$$

Géométrie sur une image

Transformations géométriques d'une image

(suite de l'article paru dans la feuille de vigne n° 124)

Alain MASCRET
mascret.alain@gmail.com

Résumé : Insérer une image dans une figure obtenue grâce à un logiciel de géométrie dynamique. Transformations géométriques d'une image. Activités géométriques en collège.

Mots clés : Géométrie dynamique, *geowiki*, *geogebra*, *geonext*, *carmetal*, distorsion, traitement d'image, agrandissement, réduction, théorème de Thalès, transformation géométrique, homothétie, similitude, affinité, transvection, motivation des élèves à la géométrie par le travail sur une photographie.

Dans l'article précédent, publié dans la feuille de vigne n°124, nous avons tracé une figure sur une image sans la modifier. Cette fois, nous allons nous intéresser aux transformations géométriques que l'on peut faire subir à une image. Ces transformations peuvent être montrées aux élèves de collège. Ils les rencontrent en manipulant des images en dehors de nos cours. Pourquoi ne pas en profiter ?

1) Agrandissement ou réduction d'une photographie :

Le théorème de Thalès est souvent perçu comme abstrait par nos élèves de quatrième. L'agrandissement ou la réduction sans déformation d'une photographie en donne une application concrète.

Dans le triangle ABC, plaçons D sur [AB] et traçons la parallèle à (BC) passant par D. Elle coupe [AC] en E. Nous obtenons ainsi une « situation de Thalès ».

Dans la fenêtre « Algèbre », *geogebra* indique les longueurs des segments :

BC = a = 9,25 DE = e = 5,44

En utilisant la ligne de saisie, au bas de la figure, entrons $r=e/a.$

$r=\frac{e}{a}=0{,}59$ est le rapport de réduction.

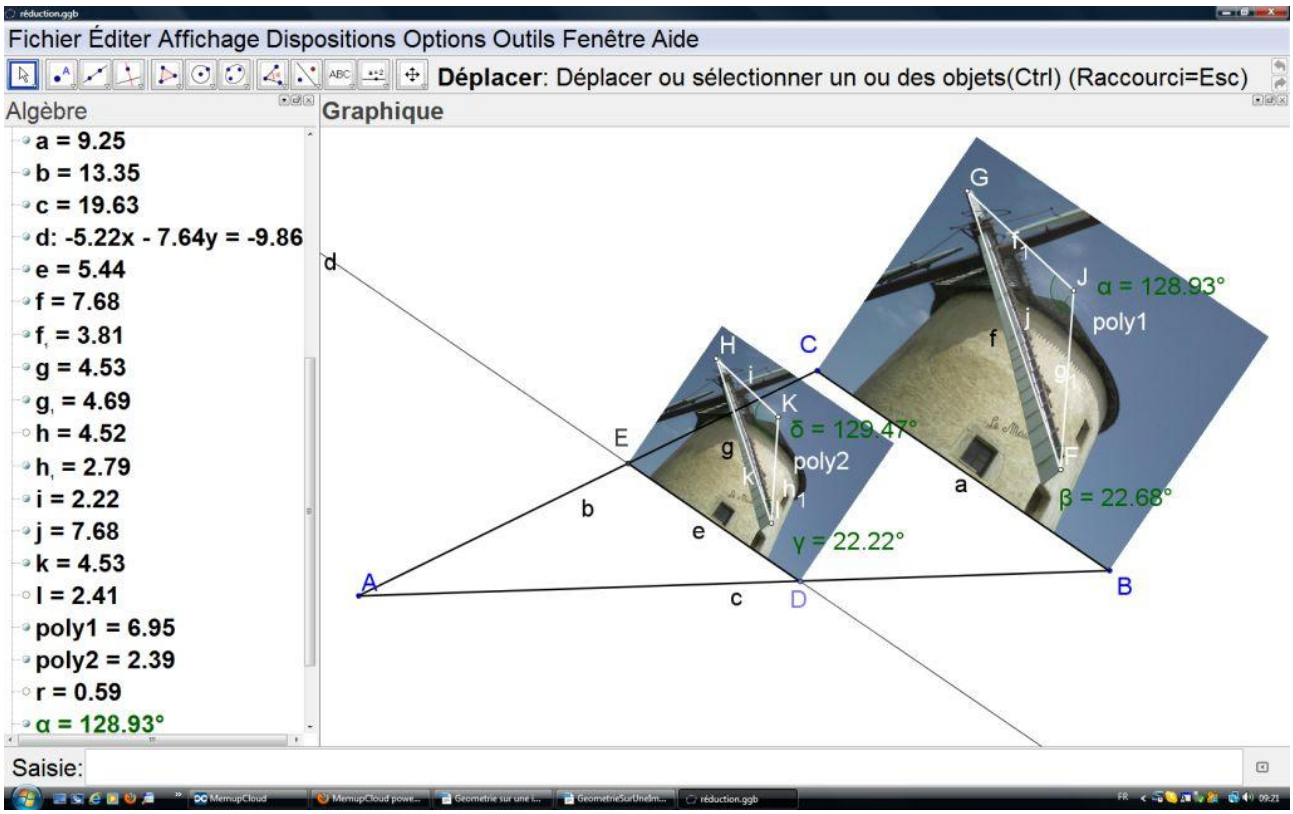


Figure 5
Le moulin de Bouhy © Photo Irène Mascret

Insérons deux fois la même photographie en utilisant les coins C et B pour la première et E et D pour la seconde. Cette seconde image est une réduction de rapport *r* de la première, ce que nous pouvons vérifier.

Traçons, par exemple le segment [GF] de longueur f = 7,68 sur l'aile du moulin de la grande photographie. Le segment qui lui correspond sur la petite photographie est [HI] de longueur g = 4,53. Calculons r × f. *Geogebra* répond en écrivant h = 4,52. L'écart entre g et h est dû au manque de précision du tracé, fait à la souris.

Traçons maintenant le triangle GFJ sur la grande photographie et son correspondant HIK sur la petite. Geogebra les désigne respectivement par poly1 et poly2 dans la fenêtre « algèbre » et nous en donne les aires. Calculons cette fois $r^2 \times f$. Nous obtenons l = 2,41 au lieu de 2,39 indiqué pour l'aire de HIK.

Geogebra permet aussi de mesurer les angles. Dans notre exemple, l'écart ne dépasse pas 1°.

$$\widehat{JFG} = 22{,}68° \text{ et } \widehat{KIH} = 22{,}22°$$
$$\widehat{GJF} = 128{,}93° \text{ et } \widehat{HKI} = 129{,}47°$$

Cette activité permet de rendre sensible aux élèves que l'absence de déformation d'une image correspond à une transformation géométrique qui conserve les angles et qui modifie les longueurs en les multipliant par un même nombre. Les longueurs correspondantes sur les deux images sont proportionnelles. C'est également l'occasion de leur parler des incertitudes des mesures.

2) Symétrie :

Dans le même esprit, il peut être intéressant de montrer aux élèves l'effet sur une photographie des transformations géométriques qu'ils connaissent. Bien que *Geogebra* considère les images comme des objets à part entière auxquels il possible d'appliquer une transformation géométrique (symétrie, translation, rotation, homothétie), il me semble plus formateur de continuer à appliquer la méthode précédente.

Cette méthode s'applique sans difficulté à la symétrie centrale, mais pas à la symétrie axiale qui change l'orientation des angles. Il faut retourner l'image et pour cela utiliser le troisième coin.

Voici une façon de procéder :
Insérons l'image comme d'habitude.
A est le coin 1 et B le coin 2.
Plaçons le point C sur le coin 4 de l'image.

Si la position du point C est correcte, en ouvrant les propriétés de l'image et en fixant le coin 4 sur C, l'image ne doit pas bouger.

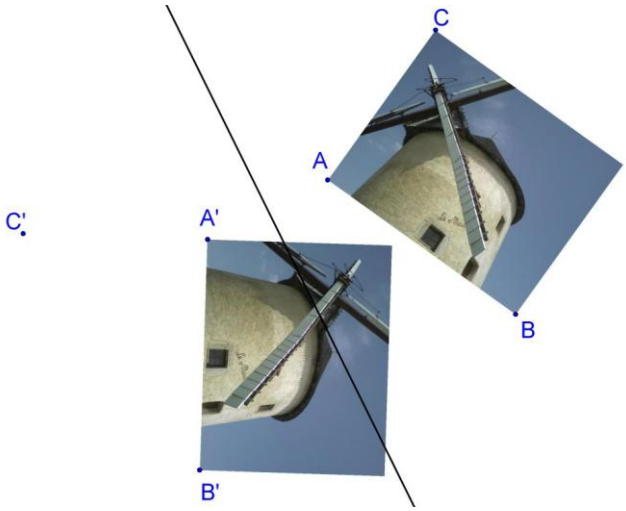


Figure 6

Les points A', B' et C' sont les symétriques des points A, B et C par rapport à l'axe tracé.

Insérons à nouveau la même image en choisissant A' pour coin 1 et B' pour coin 2.

Regardons au passage ce que nous obtenons (figure 6). La transformation géométrique est pour l'instant un déplacement (ici une rotation) puisque l'image n'a pas encore été retournée.

Terminons la manipulation en choisissant le point C' pour coin 4. Cette fois nous obtenons bien deux images symétriques. (figure 7).

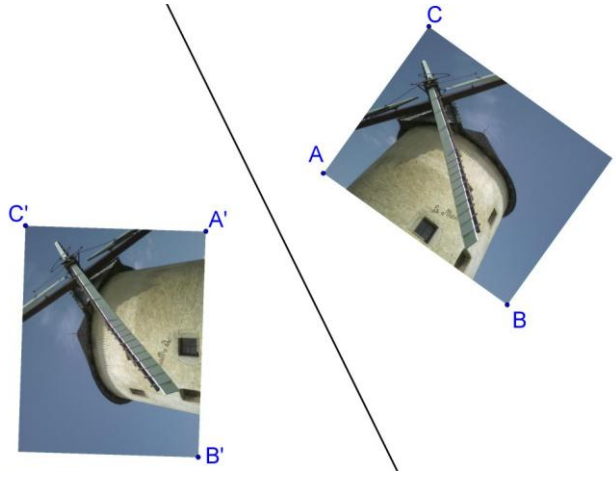


Figure 7

Cette activité fait sentir concrètement l'importance de la conservation de l'orientation.

3) Déformations de l'image :

L'utilisation du troisième coin permet de déformer la photographie et, par là même de montrer des transformations géométriques qui « transforment vraiment ».

Reprenons notre image. Choisissons à nouveau comme coins les points A et B. Nous les laisserons fixes et déplacerons le point C choisi pour coin 4.

Un déplacement quelconque du point C peut être obtenu par un déplacement sur une droite perpendiculaire à (AB) suivi d'un déplacement sur une droite parallèle à (AB). Il suffit donc d'examiner les transformations géométriques correspondant à ces deux façons de déplacer le point C. En composant ces transformations, nous obtiendrons toutes les déformations possibles de l'image.

Bien que déformées, ces nouvelles images restent très reconnaissables. Ces transformations conservent donc certaines propriétés de l'image initiale. Il est naturel de rechercher lesquelles et cette recherche peut donner lieu à des exercices.

a) C se déplace sur une perpendiculaire à la droite (AB) :

Observons la transformation de la photographie. Appelons S_1 le sommet du moulin sur la photographie de départ et S son image sur la photographie transformée. Nous constatons que :

(S_1 S) est perpendiculaire à (AB)

$\frac{S_1H}{SH}=\frac{C_1A}{CA}=k$, H étant le projeté orthogonal de S_1 sur (AB).

Cette proportion nous fait penser au théorème de Thalès et nous incite à tracer les droites (C_1S_1) et (CS) qui se coupent en I sur (AB). Nous admettons que l'image d'une droite est une droite. Si une droite coupe la droite (AB) dont les points sont invariants, son image coupe la droite (AB) au même point. Ce raisonnement a déjà été fait pour la symétrie axiale. Nous disposons de cette façon d'une construction de l'image d'un point.

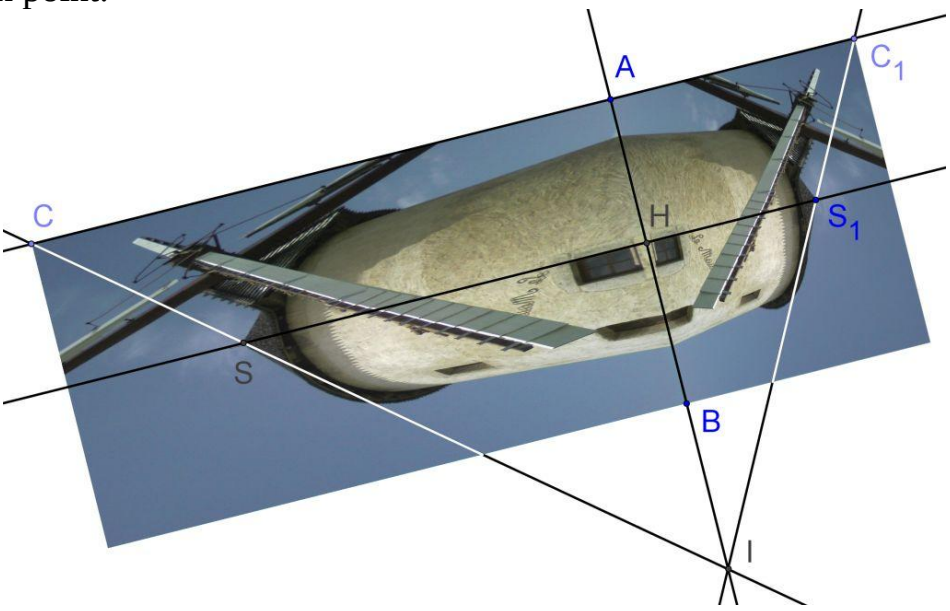


Figure 8
Quand C se déplace sur une perpendiculaire à la droite (AB),
la photographie est transformée par une affinité orthogonale d'axe (AB)

Quelles sont les propriétés conservées par cette transformation ?

Observons que si C et C_1 sont de part et d'autre de la droite (AB), comme sur la figure 8, la transformation change l'orientation. S'ils sont du même côté de (AB), elle la conserve.

Les longueurs ne sont pas conservées mais obtenir CS en fonction de C_1S_1 peut se faire en utilisant la définition du cosinus :

$$CS = C_1S_1 \frac{\cos \widehat{AIC_1}}{\cos \widehat{AIC}}$$

La conservation des milieux se montre en utilisant le théorème de la droite des milieux.

Sur la figure 9, M_1 étant le milieu de $[R_1S_1]$, une première application de ce théorème dans le triangle RR_1S_1 prouve que L est milieu de $[RS_1]$. Une seconde application dans le triangle RS_1S montre que M est milieu de [RS].

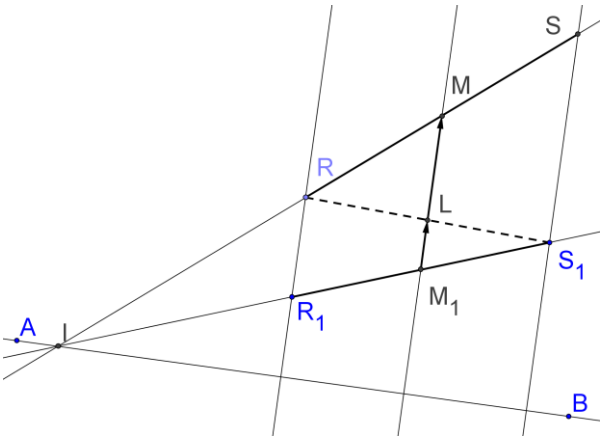


Figure 9

La conservation des milieux entraine celle du parallélisme en raison de la propriété caractéristique du parallélogramme.

Les aires sont multipliées par k. Il suffit de le montrer pour un triangle, puisque tout polygone peut être considéré comme « somme » de triangles du point de vue de l'aire.

Nous partageons le triangle $R_1S_1T_1$ en deux, en traçant une parallèle à (AB) passant par le sommet T_1 coupant le côté opposé $[R_1S_1]$ en G_1. (Figure 10). R_1 se projette orthogonalement sur cette droite en E_1 et S_1 en F_1.

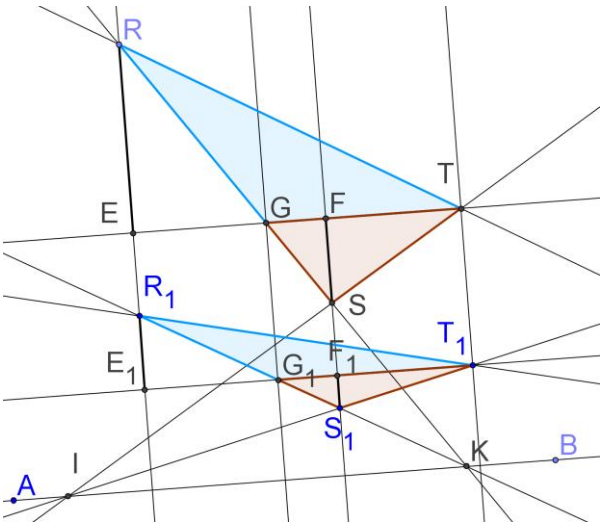


Figure 10

Les images respectives E, F, G, et T de E_1, F_1, G_1 et T_1 sont sur la parallèle à (AB) passant par T, à l'intersection de la perpendiculaire à (AB) passant respectivement par E_1, F_1 G_1 et T_1.

Comme $GT = G_1T_1$ et $FS = k \times F_1S_1$,
l'aire de GST vaut k fois celle de $G_1S_1T_1$.
Le même raisonnement s'applique à RGT
et $R_1G_1T_1$ et finalement à RST.

b) C se déplace sur une parallèle à la droite (AB) :

La photographie transformée a maintenant la forme d'un parallélogramme ABDC, en appelant D le troisième coin. Observons, comme précédemment le point S_1 et son image S.

La droite (S_1S) est parallèle à la droite (AB). Elle coupe $[AC_1]$ en K_1 et [AC] en K. Le point K est l'image de K_1.

Le parallélogramme AH_1SK est l'image du rectangle $AH_1S_1K_1$, H_1 étant le projeté orthogonal de S_1 sur (AB) ce qui nous donne une méthode de construction de l'image d'un point.

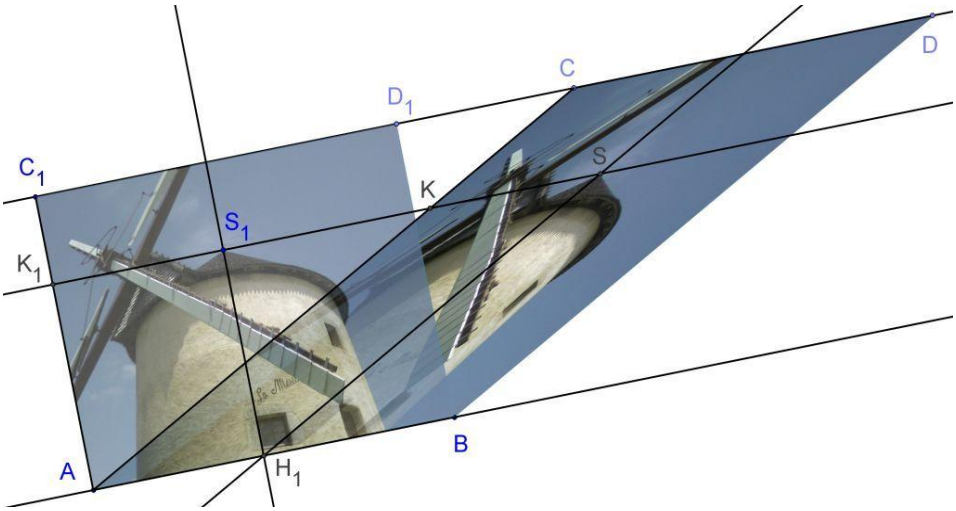


Figure 11
Quand C se déplace sur une parallèle à la droite (AB),
la photographie est transformée par une transvection d'axe (AB).

Quelles sont les propriétés conservées par cette transformation ?

Ici C_1 et son image C sont toujours du même côté de la droite (AB). La transformation conserve l'orientation.

Les longueurs et les angles ne sont visiblement pas conservés.

Comme au paragraphe précédent nous admettons que l'image d'une droite est une droite. Si une droite coupe la droite (AB) dont les points sont invariants, son image coupe aussi la droite (AB) au même point, ce qui permet de construire d'une autre façon l'image d'un point.

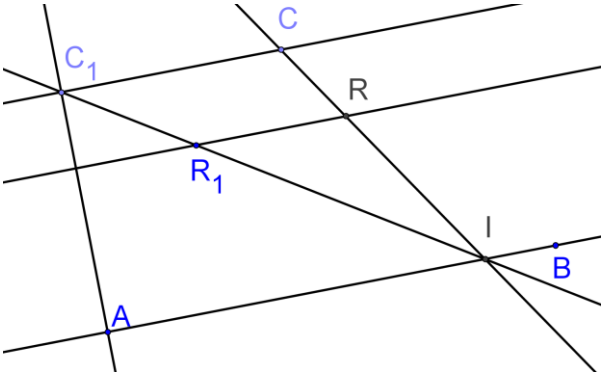


Figure 12

La figure 12 montre la construction de l'image R de R_1, connaissant l'image C de C_1.

Ici encore la conservation des milieux peut se montrer grâce au théorème de la droite des milieux, comme le montre la figure 13.

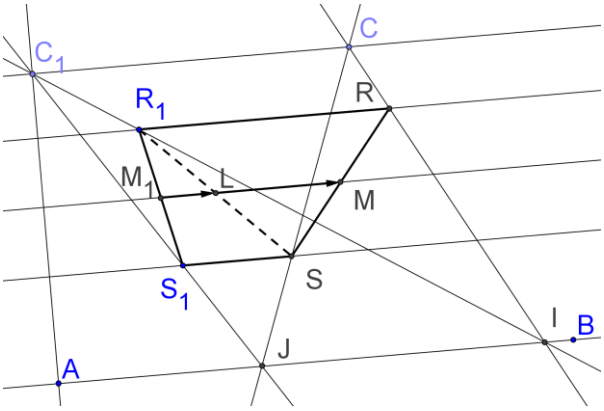


Figure 13

Enfin, une propriété qui surprend beaucoup les élèves, la transformation conserve les aires bien qu'elle ne conserve pas les longueurs.

Sur la figure 14, les triangles $R_1S_1T_1$ et RST sont partagés en deux triangles par la parallèle à (AB) passant par S_1 qui coupe $[R_1T_1]$ en U_1 et [RT] en U.

U est l'image de U_1 et S l'image de S_1 donc

$U_1S_1 = US$. (car sur une droite parallèle à (AB) les longueurs se conservent)

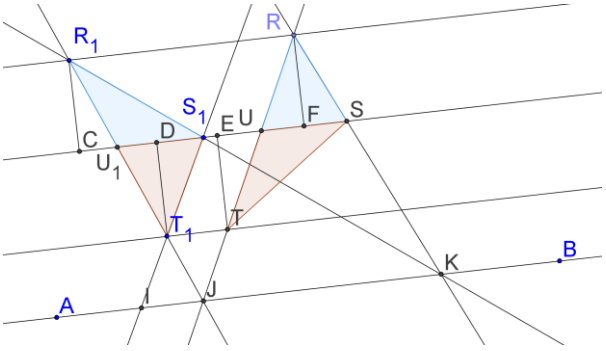


Figure 14

C, D, E et F sont les projetés orthogonaux respectivement de R_1, T_1, T et R.

$R_1C = RF$ et $T_1D = TE$

Les triangles $R_1U_1S_1$ et RUS ont donc la même aire et il en est de même des triangles $T_1U_1S_1$ et TUS.

Comme tout polygone peut être considéré du point de vue de l'aire comme une « somme » de triangles, la

transformation conserve les aires.

Les démonstrations suggérées ci-dessus sont toutes du niveau de quatrième. Il ne s'agit pas, bien sûr de faire la théorie de ces transformations, mais de résoudre certains problèmes qui se posent de façon naturelle pendant la manipulation.

4) Sitographie :

Pour terminer, voici quelques liens en rapport avec cet article et le précédent:

Sur l'astronomie le site du CLEA (comité de liaison enseignants astronomes)
http://www.ac-nice.fr/clea/

Le site du musée des beaux-arts de Dijon
(en attendant de le visiter réellement lors d'un passage à Dijon)
http://mba.dijon.fr/

Sur Zanobi Machiavelli :
http://www.treccani.it/enciclopedia/zanobi-machiavelli_(Dizionario_Biografico)/
C'est en italien, mais la traduction de google est compréhensible.

Sur l'utilisation des logiciels de géométrie dynamique :
http://geowiki.u-bourgogne.fr/
Créé par l'IREM de Dijon, ce wiki voudrait être un lieu d'échange pour tous ceux qui utilisent des logiciels de géométrie dynamique, libres ou gratuits. Je vous invite donc à le visiter et surtout à vous y exprimer

Multiplications
Techniques avec les doigts

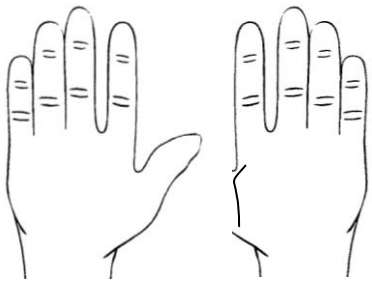
Marie-Noëlle RACINE
mnracine@wanadoo.fr

Résumé : dans son ouvrage *nouveaux elemens de geometrie* publié en 1667, Antoine Arnauld décrit une technique de multiplication de *nombres digites*, c'est-à-dire utilisant les doigts des deux mains pour calculer facilement le résultat de multiplications de deux nombres compris entre 5 et 10.

Mots clés : multiplication, calcul avec les mains.

Pour effectuer des multiplications, la plupart du temps, il faut « savoir ses tables de multiplication ! »
Pour cela, on peut parfois compter avec les doigts des mains !

On connaît (tous ?) la manière d'afficher avec les doigts des deux mains les résultats de la « table du 9 ». Revoyons la méthode sur un exemple (elle s'applique de la même façon pour les 10 résultats de cette table) :



$6 \times 9 = 54$

Puisqu'on veut le résultat de 6×9, on replie le sixième doigt et on compte, à gauche le nombre de dizaines (ici 5), à droite le nombre d'unités (ici 4).

Antoine ARNAULD, a révélé (et justifié) dans son ouvrage *NOUVEAUX ELEMENS DE GEOMETRIE*, publié à Paris en 1667, au livre I, pages 14 et 15, la manière de

faire apparaître sur les doigts des deux mains, moyennant une petite multiplication connue, les résultats de tous les produits de deux nombres compris entre 5 et 10.

NOVVEAVX ELEMENS
DE
GEOMETRIE;
CONTENANT,
Outre un ordre tout nouveau, & de nouvelles demonſtrations des propoſitions les plus communes,
De nouveaux moyens de faire voir quelles lignes ſont incommenſurables,
De nouvelles meſures des angles, dont on ne s'eſtoit point encore aviſé,
Et de nouvelles manieres de trouver & de demontrer la proportion des Lignes.
Antoine Arnauld

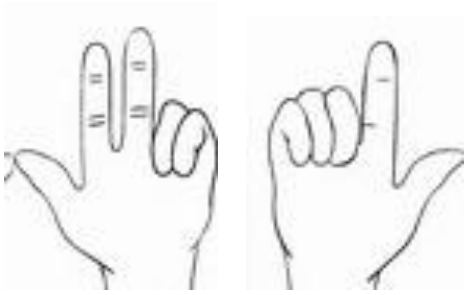
A PARIS,
Chez Charles Savreux, Libraire Juré, au pied de la Tour de Noſtre-Dame, à l'Enſeigne des trois Vertus.
M. DC. LXVII.
AVEC PRIVILEGE DV ROY.

Description de la méthode, suivie d'un exemple :
Livre I paragraphe LXIII

C'est ſur cela auſſi qu'eſt fondée une invention fort aiſée de trouver les multiplications des nombres depuis 5 juſqu'à 10. Il ne faut que baiſſer les 10 doigts, puis relever d'une main autant de doigts qu'il s'en faut que l'un des nombres qu'on veut multiplier n'aille juſqu'à 10; comme ſi ce nombre eſt 8, en relever 2, & de l'autre de même autant qu'il s'en faut que l'autre nombre n'aille juſqu'à dix; comme ſi ce nombre eſt 7, en relever 3: cela fait il faut conter autant de dixaines qu'il y a de doigts baiſſez, & multiplier les doigts levez d'une main par ceux de l'autre, en ne les prenant que pour des unitez, & on aura le nombre qu'il faut.	C'est sur cela aussi qu'est fondée une invention fort aisée de trouver les multiplications des nombres depuis 5 jusqu'à 10. Il ne faut que baisser les dix doigts, puis relever d'une main autant de doigts qu'il s'en faut que l'un des nombres qu'on veut multiplier n'aille jusqu'à dix ; comme si ce nombre 8, en relever deux, & de l'autre de même autant qu'il s'en faut que l'autre nombre n'aille jusqu'à dix ; comme si ce nombre est 7, en

	relever trois : cela fait il faut conter autant de dixaines qu'il ya de doigts baissez, & multiplier les doigts levez d'une main par ceux de l'autre, en ne les prenant que pour des unitez, & on aura le nombre qu'il faut.

On le voit, il suffit de connaître les résultats des multiplications de nombres compris entre 1 et 5 pour pouvoir appliquer cette méthode :



Pour connaître le produit de 8 par 7, on baisse tous les doigts, on relève d'une main autant de doigts qu'il en faut pour aller de 8 à 10, et de l'autre autant de doigts qu'il en faut pour aller de 7 à 10. C'est-à-dire, on relève 2 doigts d'une main et 3 de l'autre. On compte le nombre de doigts baissés pour obtenir le nombre de dizaines (ici 5) et on multiplie le nombre de doigts levés d'une main par ceux de l'autre (ici 2 × 3 = 6), pour avoir le nombre d'unités.
On a 7 × 8 = 5 dizaines + 6 unités = 56.

Continuons avec le texte d'Antoine ARNAULD que nous commenterons au fur et à mesure, pour connaître sa justification :

La raiſon de cela eſt qu'on ne fait en cela que multiplier

par { 10. — 2. / 10. — 3. } 100 — 20 — 30 + 6. ſomme 56.

Arnauld continue :

Car en baiſſant tous les doigts, on fait la premiere multiplication partiale qui donne dix dizaines.

En levant deux doigts d'une main on fait ce que doit faire la ſeconde multiplication partiale, qui eſt de + 10. par — 2, ce qui donne — 20 : car en levant deux doigts on oſte deux dizaines.

En levant 3 doigts de l'autre main on fait encore ce que doit faire la troiſiéme multiplication partiale, qui eſt de + 10 par — 3, ce qui donne — 30 : car en levant 3 doigts on oſte trois dizaines.

[…]

En fait, au XXI[e] siècle, pour ce début de justification, nous dirions qu'il développe le produit
$(10 - 2) \times (10 - 3)$ soit : $(10 - 2) \times (10 - 3) = 10 \times 10 - 10 \times 2 - 10 \times 3 + 2 \times 3$. Ce qui donne 56 comme résultat.
Il justifie la fin de ce calcul, à savoir $(-2) \times (-3) = + 6$, par :

Et enfin en multipliant les doigts levez d'une main par ceux de l'autre, on multiplie — 2 par — 3, ce qui donne + 6 par la raiſon que nous avons dite, qui eſt que les deux multiplications negatives ont oſté cela de trop. Car la premiere oſtant 2 fois 10, a oſté 2 fois 7 plus 2 fois 3. Et la ſeconde oſtant 3 fois 10, a oſté 3 fois 8, plus 3 fois 2. Et ainſi elles ont oſté deux fois 3 fois 2, qui n'en devoient eſtre oſtez qu'une fois.

Car 10 fois 10 eſt égal à

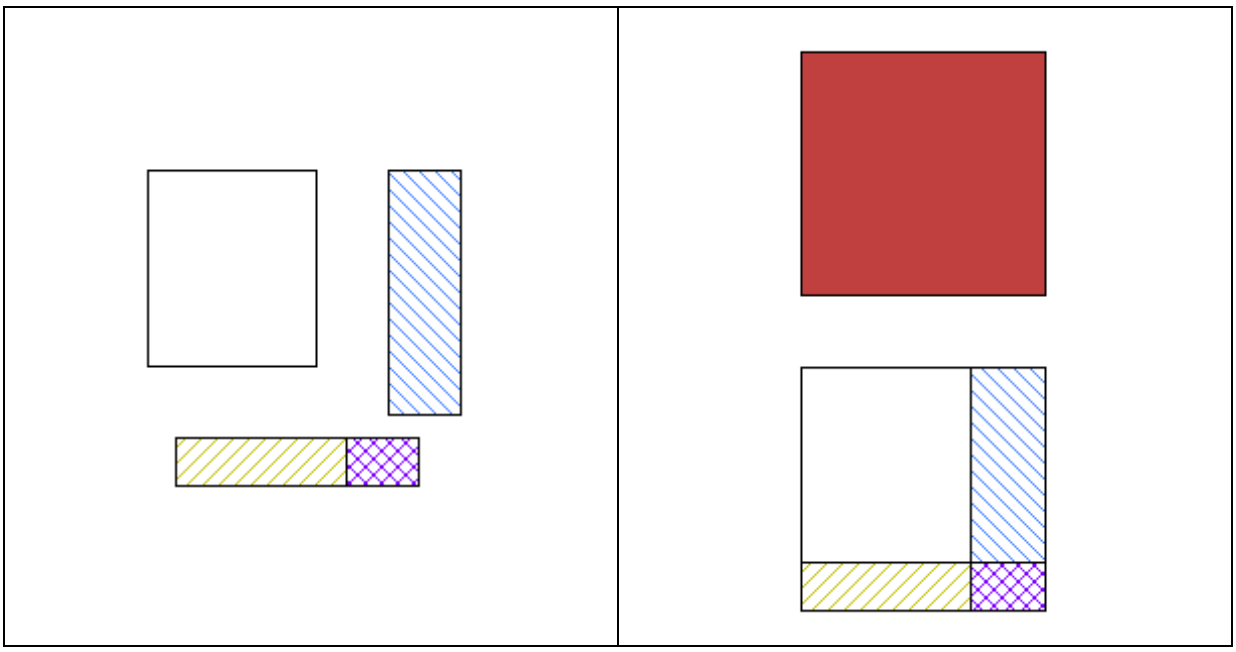
7 + 3.
par 8 + 2.

Ce qui fait 7 fois 8 + 8 fois 3 + 2 fois 7 + 2 fois 3.

Et ainſi 10 fois 10 n'eſt plus grand que 7 fois 8 (qui eſt ce que l'on cherche) que des trois dernieres multiplications, 8 fois 3, 2 fois 7, 2 fois 3. Et ainſi cette derniere n'en doit eſtre oſtée qu'une fois, & ſi on l'a oſtée deux fois, il la faut remettre une fois : comme on fait auſſi en mettant *plus* à la multiplication de moins 3 par moins deux.

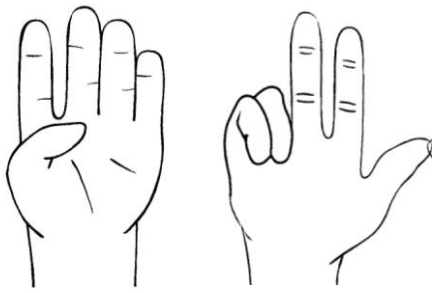
Pour comprendre ce texte, et en particulier des expressions comme « *les deux multiplications négatives ont osté cela de trop* », nous pouvons le transcrire avec l'algèbre, à la manière moderne :
$10 \times 10 = (7 + 3) \times (8 + 2)$
$10 \times 10 = 7 \times 8 + 7 \times 2 + 8 \times 3 + 2 \times 3$ ici, on a la traduction algébrique de la phrase « *Et ainsi 10 fois 10 n'est plus grand que 7 fois 8 (qui est ce que l'on cherche) que des trois dernieres multiplications, 8 fois 3, 2 fois 7, 2 fois 3.* »
$10 \times 10 = 7 \times 8 + (10 - 3) \times 2 + (10 - 2) \times 3 + 2 \times 3$
$10 \times 10 = 7 \times 8 + 10 \times 2 - \mathbf{3 \times 2} + 10 \times 3 - \mathbf{3 \times 2} + 2 \times 3$ ce qui traduit bien « *Et ainsi cette dernière* [2 fois 3] *n'en doit estre ostée qu'une fois, &t si on l'a ostée deux fois, il faut la remettre une fois* »
La phrase « *comme on fait aussi en mettant* plus *à la multiplication de moins 3 par moins deux* » n'est que la description de ce qui a été fait en appliquant ce que l'on nomme aujourd'hui la *règle des signes,* à savoir : $- \times - = +$.

Si l'on veut expliquer cette opération à l'aide de figures géométriques rectangles comme il était d'usage auparavant lorsqu'il s'agissait de trouver des *produits*, parfois appelés *rectangles* : le grand carré rouge foncé vaut 10×10. On lui enlève le rectangle bleu, hachures obliques descendant vers la droite, $(- 10 \times 3)$, on enlève encore le long rectangle ocre, hachures obliques montant vers la droite, $(- 10 \times 2)$, mais on a enlevé deux fois le rectangle violet, hachures croisées, il faut le rajouter $(+ 2 \times 3)$. On obtient le rectangle blanc 7×8 :



Voici un autre exemple, où il y a une retenue et voyons comment on en tient compte :

Soit à trouver le produit de 6 par 7 :



Après avoir baissé tous les doigts ; on relève 4 doigts de la main gauche car pour aller de 6 à 10, il manque 4 ; on relève 3 doigts de la main droite car pour aller de 7 à 10, il manque 3 ; on multiplie le nombre de doigts levés de la main gauche par le nombre de doigts levés de la main droite soit : $4 \times 3 = 12$, il y a 12 unités ; il reste 1 + 2 doigts baissés, il y a 3 dizaines.
Le résultat est donc : 3 dizaines + 12 unités soit 42. On a bien $6 \times 7 = 42$.
À noter, pour conclure, que cette technique a été décrite, sans démonstration, à des élèves de collège (tous niveaux). Certains de ces élèves utilisent désormais ce moyen des doigts des mains pour vérifier un résultat et se rassurer lorsqu'ils ont à faire une multiplication de deux nombres compris entre 5 et 10.

Annexe : biographie succincte d'Antoine ARNAULD :
Né à Paris le 6 février 1612, il décède à Bruxelles le 8 août 1694.
Prêtre, théologien, philosophe et mathématicien, ami de Pascal, il correspond avec Leibniz, Malebranche, Bossuet et bien d'autres de ses contemporains. Janséniste, il s'oppose aux jésuites et aux calvinistes. Il est ainsi forcé de se cacher durant plus de vingt ans. Après une courte réhabilitation, il fuit la France et émigre aux Pays-Bas puis s'installe à Bruxelles.

Van BIJLERT Jan Hermantz (Utrecht 1597 ; 1671), *Les quatre Evangélistes*, ≈1625, MBA Quimper, ©photo MN Racine

Comment fabriquer de grands nombres premiers ?

Michel LAFOND
mlafond001@yahoo.fr

Résumé : Une méthode simple pour obtenir des nombres premiers aussi grands que la calculette le permet, avec une preuve "rapide" de leur primalité. Cet article donne aussi des applications numériques et, pour l'anecdote, exhibe un nombre premier de 100 chiffres commençant par 2012... et se terminant par 2013.

Mots clés : Pocklington, nombres premiers.

1. Pourquoi vouloir des grands nombres premiers ?

Grand signifie ici "ayant plusieurs centaines de chiffres".
Ma réponse à la question est "pour le plaisir". Mais dans le domaine de la cryptographie, ces nombres ont une utilité certaine. Certains professionnels utilisent pour crypter leurs messages un codage basé sur un grand entier N qui est le produit de deux grands nombres premiers p et q (De tels nombres N sont appelés semi-premiers ou nombres RSA). Rivest, Shamir et Adleman ont développé un algorithme qui porte leur nom (algorithme RSA). Il permet un codage sûr tant que le nombre N qui est public reste indécomposable en temps raisonnable. L'astuce est que N suffit pour coder, mais que les deux facteurs p et q sont nécessaires pour décoder. La société "RSA data security" suit de très près l'évolution de ceux qui cherchent à factoriser les grands nombres RSA.
En 2005, l'Université de Bonn a réussi à factoriser un nombre RSA de 200 chiffres, et en 2009 Thorsten Kleinjung a réussi à factoriser un nombre RSA de 232 chiffres ce qui lui a valu un prix de 50 000 $, mais ces réussites sont exceptionnelles car on est très loin aujourd'hui de savoir factoriser à coup sûr un entier $N = pq$ de 200 chiffres.
Tout cela pour dire que des gens ont besoin d'avoir à leur disposition de grands nombres premiers, avec **une certitude** quant à leur primalité.

2. Comment être sûr qu'un nombre déclaré premier l'est vraiment ?

Pour tester la primalité de N, tout le monde connaît la méthode des divisions successives consistant à tester la divisibilité de N par tous les nombres premiers 2, 3, 5, 7, 11 … jusqu'à la racine carrée de N.

Si N vaut environ 10^6 la méthode précédente nécessite l'essai des diviseurs premiers jusqu'à 1000. Il y en a 168, ce n'est pas beaucoup.
Si N vaut environ 10^{12} la méthode précédente nécessite l'essai des diviseurs premiers jusqu'à un million. Il y en a environ 72000, ça ne va plus du tout. D'autant plus qu'il faudrait disposer d'une table FIABLE des nombres premiers jusqu'à un million.
Évaluons le temps de calcul en supposant connue la table des nombres premiers jusqu'à 10^6 :
À raison de 5 minutes par division, cela représenterait deux bonnes années de travail (à 8 heures par jour) sans vacances.
Ne parlons pas des entiers de l'ordre de 10^{100} ou 10^{500} qui nous intéressent ici.
Les logiciels comme MAPLE qui vous disent par exemple : 1 000 000 000 000 000 000 001 est premier, ne sont pas exempts de bugs. De plus certains algorithmes prouvant la primalité sont très compliqués (celui de LENSTRA fait appel aux courbes elliptiques voir QUADRATURE N° 34), d'autres utilisent beaucoup de mémoire, autant de sources potentielles d'erreurs.
Pire pour un mathématicien, certains algorithmes dits heuristiques donnent un résultat "presque certain" c'est-à-dire que si N est déclaré premier par ces algorithmes, il y a une probabilité (extrêmement faible) que N soit en fait composé !
Le théorème qu'on va voir ci-dessous permet d'obtenir des nombres premiers aussi grands que l'on veut. Pour l'ordre de grandeur 10^{100}, on a en plus la possibilité de vérifier humainement (à la main) la primalité en un temps raisonnable. De plus aucune table de nombres premiers (au-delà de 100) n'est requise. Que pourrait-on exiger de plus ?

Le théorème magique qui va permettre ce miracle est :

3. Le théorème de POCKLINGTON. (1916)

Toutes les lettres désignent des entiers naturels.
Si $N - 1 = q^n R$ avec q premier et $n \geq 1$
et s'il existe $a > 0$ tel que :

1) $a^{N-1} \equiv 1 \mod N$

2) PGCD $(a^{\frac{N-1}{q}} - 1, N) = 1$

alors : tout facteur premier p de N est de la forme $k\,q^n + 1$

On voit bien l'intérêt d'un tel théorème : on aura à tester q^n fois moins de diviseurs que par la méthode naïve. Pour peu que q^n soit assez grand le gain sera donc considérable.
Et si q^n est supérieur à la racine carrée de *N*, il n'y a même pas de facteur à tester !

Démonstration du théorème :

Sous les hypothèses du théorème, soit p un facteur premier de N.

$a^{N-1} \equiv 1 \mod N \quad \Rightarrow \quad a^{N-1} \equiv 1 \mod p$ (1)

donc a est premier avec p. Cela entraîne $a^{p-1} \equiv 1 \mod p$ (2)

Soit e l'ordre de a modulo p, c'est-à-dire le plus petit entier positif t tel que $a^t \equiv 1 \mod$ p.
On sait que $a^t \equiv 1 \mod p$ si et seulement si t est multiple de e.

D'après (1) et (2) e divise $N-1$ et e divise $p-1$ (3)

Or par hypothèse $\frac{N-1}{q}$ est entier et $a^{\frac{N-1}{q}} \not\equiv 1 \mod$ p

(Sinon p serait facteur commun à $a^{\frac{N-1}{q}} - 1$ et N ce qui est contraire à l'hypothèse 2).
Donc e ne divise pas $\frac{N-1}{q}$ donc q ne divise pas $\frac{N-1}{e}$ (qui est entier d'après (3)).

Si on remplace N – 1 par $q^n R$, on a donc : q ne divise pas $\frac{q^n R}{e}$.

Posons $\frac{q^n R}{e} = u$ c'est à dire $q^n R = u\, e$.
q premier, ne divise pas u donc q est premier avec u ainsi que q^n.
Mais q^n, premier avec u, divise $u\, e$ donc q^n divise e.

Ainsi q^n divise e et e divise $p-1$ d'où l'on déduit q^n divise $p-1$ autrement dit $p - 1 = k\, q^n$ ou encore $p = k\, q^n + 1$. C Q F D.

4. Applications.

Commençons doucement.
On souhaite par exemple un nombre premier de l'ordre de 10^{12}.
Puisque N sera choisi tel que $N - 1 = q^n R$, nous prendrons q^n et R de l'ordre de $\sqrt{N}$.

Choisissons d'abord q premier dans la table des nombres premiers inférieurs à 100.
Allons-y pour $q = 5$.

Choisissons n pour que q^n soit de l'ordre de $\sqrt{N}$ soit ici :

$$5^n \approx 10^6 \text{ ou } n \approx 8{,}58\ldots\ldots$$

$n = 9$ fera l'affaire.
$N - 1 = q^n R$ devra être pair, donc R aussi.
On va donc imposer à R d'être pair et légèrement inférieur à $q^n = 5^9 = 1\ 953\ 125$.
Pourquoi prendre $R < q^n$?
Parce que dans ce cas, si on trouve un nombre a qui vérifie les deux hypothèses du théorème, on aura comme conclusion que tout facteur premier p de N est de la forme $k\,q^n + 1$.
Mieux, les hypothèses et le fait que $R < q^n$ suffisent en fait pour avoir N premier, sinon N aurait un facteur premier $p = k\,q^n + 1$ inférieur ou égal à $\sqrt{N}$ et cela entraînerait :

$$q^n < k\,q^n + 1 = p \le \sqrt{N} = \sqrt{q^n R + 1} \qquad (4)$$

Divisons les deux membres de (4) par $\sqrt{q^n}$. On obtiendrait : $\sqrt{q^n} < \sqrt{R + 1/q^n}$ soit en élevant au carré : $q^n < R + 1/q^n$ donc $q^n \le R$ ce qui est en contradiction avec $R < q^n$.

Cela se précise :
Pour le nombre a du théorème, nous prendrons $a = 2$ [Cela n'a pas d'importance].
Le seul degré de liberté qui reste est le choix de R. Le travail à faire est donc le suivant :

> Balayer les valeurs paires de R depuis $q^n - 1 = 1\ 953\ 124$ en décroissant.
> Pour chaque valeur de R, poser $N = 1 + q^n R = 1 + 5^9 R$.
> Si $2^{N-1} \equiv 1 \mod N$ et PGCD $(2^{\frac{N-1}{5}} - 1, N) = 1$ alors N est premier.

Le programme en annexe fonctionne une fraction de seconde et donne pour $R = 1\ 953\ 114$ le nombre premier $N = 1 + q^n R = 3\ 814\ 675\ 781\ 251$.

Vérifier à la main, par la méthode des divisions successives nécessiterait disons 4 ans, mais en annexe figure une preuve nécessitant moins de 120 multiplications et tout à fait exécutable à la main en une journée !

Voulez-vous un nombre premier de 200 chiffres ?
La même technique et le même programme exécuté avec $q = 83$ et $n = 52$ donne le nombre premier de 200 chiffres ci-dessous décomposé en 4 tranches de 50 chiffres :

38381470267922467264441665594985762925284275145909
88706567736712230410269996048771200754839846435950
00718909794532108160942122820849529565415233502809
35902334467934772554430386153929473554154963932089.

Voulez-vous un nombre premier de 100 chiffres commençant par 2012 et se terminant par 2013 ? Pas de problème. Deux petites modifications au programme (on se place au voisinage de 2012×10^{96} et on filtre pour ne garder que les nombres

premiers congrus à 2013 modulo 10 000) permettent de trouver en quelques secondes que :

2012573273162587865667865637253743574534625566376607583799726818493315009313799550180168722135402**013** est premier.

5. Annexe.

Ce qui est difficile, ce n'est pas d'obtenir de grands nombres premiers, c'est de les CERTIFIER premiers.

Détaillons avec le nombre $N = 3\,814\,675\,781\,251$ vu plus haut.
Ce que nous devons faire pour certifier la primalité de N est de s'assurer de deux choses :

$2^{N-1} \equiv 1 \mod N$ et PGCD $(2^{\frac{N-1}{5}} - 1, N) = 1$

c'est-à-dire $2^{3814675781250} \equiv 1 \mod 3814675781251$ et
PGCD $(2^{762935156250} - 1 ; 3814675781251) = 1$

Cela paraît insurmontable, mais une astuce nommée "exponentiation rapide" permet de le faire.
D'abord, tous les calculs étant faits modulo N, on n'aura jamais à manipuler de grands nombres. Tout au plus, lors de multiplications, on rencontrera des nombres de l'ordre de N^2 qui n'a guère que 26 chiffres.
Ce qui effraie, ce sont les exposants. Mais pour calculer disons $y = x^e$ il suffit de remarquer que :

Si e est pair alors $y = (x^{\frac{e}{2}})^2$ [Une multiplication]

Si e est impair alors $y = x \times (x^{\frac{e-1}{2}})^2$. [Deux multiplications]

Au prix d'une ou deux multiplications, on a divisé l'exposant par 2 !
Les choses ne vont donc par traîner.

L'algorithme d'exponentiation rapide qui ne fait que traduire la remarque ci-dessus est le suivant :

Soit à calculer $Y = X^E$ X, E connus, E entier positif.

```
Soit Y = 1.
   Tant que E > 0 faire
      Si E impair faire Y = Y . X fin Si
      Faire X = X . X
      Faire E = partie entière (E / 2)
   fin Tant que
```

La validation de l'algorithme est dans la remarque que la quantité $Z = Y \cdot X^E$ est invariante lors de l'exécution de l'algorithme.
[Examiner les deux cas E pair, E impair].
Au début cette quantité vaut $Z = X^E$ (puisque $Y = 1$).
A la fin $E = 0$ donc $Z = Y$ et $X^E = Y$. D'où par transitivité $Y = Z = X^E$.
Ainsi pour calculer $Y = 3^{10}$ l'exécution pas à pas donne :

	$Y = 1$	$X = 3$	$E = 10$
E pair		$X = 3 \times 3 = 9$	$E = 5$
E impair	$Y = 1 \times 9 = 9$	$X = 9 \times 9 = 81$	$E = 2$
E pair		$X = 81 \times 81 = 6561$	$E = 1$
E impair	$Y = 9 \times 6561 = 59049$	$X = 6561 \times 6561$	$E = 0$

C'est fini et $Y = 3^{10} = 59049$.

Bien sûr, on peut faire toutes les multiplications modulo *N*.

Passons à la certification manuelle de la primalité de $N = 3814675781251$. Rappelons qu'on doit vérifier que :

$$2^{3814675781250} \equiv 1 \mod 3814675781251 \quad \text{et}$$
$$\text{PGCD}\,(2^{762935156250} - 1 ; 3814675781251) = 1$$

Puisque $\left(2^{\frac{N-1}{5}}\right)^5 = 2^{N-1}$ on va déjà calculer $y = 2^{\frac{N-1}{5}} = 2^{762935156250}$ modulo *N*.
On utilise l'algorithme d'exponentiation rapide avec $X = 2$ et $E = 762935156250$.
Tous les calculs sont faits modulo $N = 3814675781251$.
Le tableau ci-dessous montre tous les résultats intermédiaires de l'exécution.

Détail du calcul de $y = 2^{762935156250} \mod N$ (explications page suivante)

Y	**X**	**E**	***Facteur f*** YX – f *N*	***Facteur g*** XX – g *N*
1	2	762935156250		
1	4	381467578125		
4	16	190733789062		
4	256	95366894531		
1024	65536	47683447265		
67108864	4294967296	23841723632		4835730
67108864	1958040653386	11920861816		1005045623839
67108864	1337798422407	5960430908		469162969967

67108864	1752824984932	2980215454		805414563120
67108864	1147174981504	1490107727	20181429	344986183270
1380617863777	2414826231246	745053863	873980496366	1528671389525
2408512542276	1428753916741	372526931	902087602099	535127458180
2814294196667	1095029477901	186263465	807862917205	314335903293
3383920032512	2673088806258	93131732		1873135274368
3383920032512	3262824688196	46565866		2790807281244
3383920032512	889642578172	23282933	789183541324	207478685550
1293198611740	3146316238534	11641466		2595058254103
1293198611740	520785246303	5820733	176549409741	71098381178
561482831229	1007831474131	2910366		266267525340
561482831229	929582804821	1455183	136825464349	226526247726
2137567434410	840768656815	727591	471127771726	185308522878
2459473294924	395788983847	363795	255180909733	41064805691
730218276645	3404891019968	181897	651775876992	3039126657851
55967170368	223376969423	90948		13080343738
55967170368	817101296691	45474		175022614591
55967170368	2598010716140	22737	38116819542	1769392752682
2914833332478	1209880934418	11368		383731661459
2914833332478	1317745493515	5684		455203347611
2914833332478	3028957613864	2842		2405075752879
2914833332478	3160187538867	1421	2414732077741	2617990585175
2647116188435	60852089764	710		970718624
2647116188435	3263817857072	355	2264859605637	2792506523489
1367510850433	3147163108445	177	1128216379497	2596455426130
3092580795938	1338960829395	88		469978631333
3092580795938	2658813528442	44		1853182232097
3092580795938	1102459934017	22		318616306026
3092580795938	3728744637763	11	3022915896648	3644749218788
871459660046	2240258300381	5	511785233875	1315644510889
414637199901	1880973203022	2		927486474178
414637199901	2144441895806	1	233090682934	1205510325960
3806252644772	420693813676	0		

À la fin (en bas à gauche du tableau), on a : $y = 2^{\frac{N-1}{5}} \bmod N = 3806252644772$.

Explication et évaluation du temps de calcul :
On ne compte pas les divisions par 2 qui permettent d'avoir la colonne E. Pour les colonnes X et Y, on a des multiplications à faire MODULO *N*.
Pour un humain, la division avec des grands nombres n'est pas folichonne. Regardons de près ce qui se passe :

La première multiplication à vérifier qui est véritablement modulo N (ligne 7 du tableau) est :
4294967296 × 4294967296 = 1958040653386 modulo 3814675781251.
Comme il ne s'agit que de vérifier, on fait faire le gros du calcul à une machine qui nous donne le quotient g = 4835730 et le reste 1958040653386 de la division de XX par N.
À la main il n'y a qu'à constater que :
X X – g N = 18446744073709551616 – 4835730 N = 1958040653386
Soit deux multiplications et une soustraction.
Pour la colonne Y c'est la même chose. Ainsi à la ligne 11 du tableau, 1380617863777 provient du calcul :
Y X – f N = 67108864 × 1147174981504 – 20181429 × N.
Soit encore deux multiplications et une soustraction.

La vérification de $y = 2^{\frac{N-1}{5}} \bmod N$ = 3806252644772 [le gros du travail] nécessite donc pour l'humain vérificateur moins de 110 multiplications (on néglige les soustractions et divisions par 2) et aucune autre opération.

Il faut encore vérifier que :
PGCD ($2^{\frac{N-1}{5}} - 1, N$) = PGCD (3806252644772, 3814675781251) = 1.
Ici, deux multiplications et une soustraction suffisent grâce à M. Bezout :

3806252644772 × 1278964482833 – 1276140417825 × 3814675781251 = 1

S'il y avait un facteur commun entre 3806252644772 et 3814675781251, on le retrouverait dans la combinaison précédente.

À ce stade, la deuxième hypothèse du théorème est vérifiée.
Il ne reste plus qu'à vérifier $2^N - 1 \equiv 1 \bmod N$.
Or $2^N - 1 = \left(2^{\frac{N-1}{5}}\right)^5 - 1 = y^5 - 1$ et
$y^2 = y \times y \bmod N$ = 809533324672.
Preuve : $y \times y$ – 3797848107312 N = 809533324672.
$y^4 = y^2 \times y^2 \bmod N$ = 1278964482833.
Preuve : 809533324672^2 – 171795518501 N = 1278964482833.
$y^5 = y^4 \times y \bmod N = 1$.
Preuve : 1278964482833 × y – 1276140417825 N = 1.
Six multiplications ont suffi.

C'est terminé.
Un humain peut faire cela en une journée (moins de 120 multiplications et aucune division !).

Ci-dessous, le programme (MAPLE) qui a calculé N. Il utilise la procédure nommée "puiss" dépendant de 3 paramètres (*x*, *e*, *m*) qui calcule $y = x^e \bmod m$ par la procédure dite d'exponentiation rapide.

puiss:=proc(x,e,m) local ee,xx,y: ee:=e: xx:=x: y:=1: while ee>0 do if ee mod 2=1 then y:=y*xx mod m: fi: xx:=xx*xx mod m: ee:=floor(ee/2): od: y: end:	*calcule y = x ^ e mod m*
q:=5: e:=9: qe:=q^e: for r from qe-1 to 2 by -2 do n:=1+qe*r: n1:=n-1: nq:=n1/q: p:=puiss(2,n1,n): if p<>1 then next: fi: p:=puiss(2,nq,n)-1: if gcd(p,n)<>1 then next: fi: print (`q =`,q,`exposant `,e,`r = `,r,n,`est premier`): r:=2: od:	*balayage des valeurs de r* *test première hypothèse* *test seconde hypothèse*

Impression après exécution :
`q =`, 5, `exposant `, 9, `r = `, 1953114, `n = `, 3814675781251, `est premier`

Sitographie :
WIKIPEDIA "NOMBRE RSA" consultée le 3 juillet 2012.

MISE EN PAGE :
Céline PETITJEAN

COMITÉ DE RÉDACTION ET DE LECTURE :
Catherine LABRUERE CHAZAL
Michel LAFOND
Alain MASCRET
Marie-Noëlle RACINE
Françoise BERTRAND

RÉDACTEUR EN CHEF :
Catherine LABRUERE CHAZAL

DIRECTEUR DE LA PUBLICATION :
Catherine LABRUERE CHAZAL, Directrice de l'IREM

DÉPÔT LÉGAL :
n° 203 – 2ème semestre 2012

IMPRESSION :
Service Reprographie

FEUILLE DE VIGNE
Université de Bourgogne – UFR Sciences et Techniques
IREM
9 Avenue Alain Savary – BP 47870 – 21078 Dijon cedex
☎ 03 80 39 52 30 – Fax 03 80 39 52 39
@ : iremsecr@u-bourgogne.fr.
http://math.u-bourgogne.fr/IREM