LE NOMBRE, CET INCONNU.

Jean-Pierre Kahane

Assises de Mathématiques
Poitiers
2 avril 1999

Transcription, maquette : Jacqueline GUICHARD
Typographie LaTeX : Jean-Michel SARLAT

Juin 1999

LE NOMBRE CET INCONNU

Conférence de Jean-Pierre Kahane

J'ai donné un titre trompeur : « Le nombre cet inconnu ». Vous vous attendez à découvrir la jungle du nombre. Eh bien non ! On va se contenter de faire une ou deux promenades dans cette jungle.

C'est la PROMENADE I, la PROMENADE II, et après cela, ce sera le REPOS.

Promenade I

à travers les nombres premiers.

Contemplation.

x	$\dfrac{x}{\log x - 1}$	$\pi(x)$	$\mathrm{li}\, x$
10^3	169	168	178
10^4	1 217	1 229	1 246
10^5	9 512	9 592	9 630
10^6	78 030	78 498	78 628
10^7	661 458	664 579	664 918
10^8	5 740 303	5 761 455	5 762 209
10^9	50 701 542	50 847 534	50 849 235
10^{10}	454 011 197	455 052 511	455 055 614
	$\overset{?}{<}$	$\overset{?}{<}$	
	$\overset{?}{\sim}$	$\overset{?}{\sim}$	

$10^{10^{10^{10^3}}}$ Skewes 1933-55 $\quad 6{,}7\cdot 10^{370}$ te Riele 1986

Transparent I

PROMENADE I : A travers les nombres premiers

Contemplation du tableau

La promenade I est une promenade à travers les nombres premiers à partir de la contemplation du tableau ci-dessus [**Transparent I**].

Alors x c'est 10^3, 10^4 etc. $\frac{x}{\log(x)-1}$: je suis de la vieille école qui écrit logarithme népérien sous la forme « log ». C'est ce que vous enseignez, à juste titre, sous le sigle ln : c'est le logarithme népérien.

$\pi(x)$, j'y reviendrai tout à l'heure, c'est le nombre de nombres premiers inférieurs à x ; $\mathrm{li}(x)$, c'est le logarithme intégral de x. C'est une primitive de $\frac{1}{\log(x)}$.

Pendant que je parlais vous avez regardé le tableau, vous avez vu que $\pi(x)$, qui est naturellement la quantité à laquelle on va s'intéresser, est comprise entre $\frac{x}{\log(x)-1}$ et $\mathrm{li}(x)$, plus proche d'ailleurs de $\mathrm{li}(x)$, et d'autre part, il n'est pas difficile d'établir que $\frac{x}{\log(x)-1}$, $\frac{x}{\log(x)}$ et $\mathrm{li}(x)$ sont des quantités équivalentes.

D'où deux questions : démontrer les inégalités qui semblent évidentes sur le tableau que j'ai écrit, et d'autre part, si nous n'arrivons pas à démontrer les inégalités, au moins démontrer l'équivalence. Je vais vous faire l'histoire de la chose tout à l'heure, mais je vous dis tout de suite : cette inégalité-ci [la première du tableau] est vraie, cette inégalité-là [la seconde du tableau] est fausse. Il y a des valeurs de x très grandes pour lesquelles la seconde inégalité est inversée, pour lesquelles $\pi(x)$ dépasse $\mathrm{li}(x)$.

Est-ce qu'elles ont été découvertes par ordinateur ? Non. Si loin qu'on aille, pour le moment, dans l'exploration par ordinateur – et on est allé bien au-delà de 10^10 – on a toujours l'inégalité $\pi(x) < \mathrm{li}(x)$. C'est par un raisonnement – que je ne pourrais pas vous détailler – qui est non constructif, que Littlewood en 1914 a démontré qu'il y avait des x pour lesquels l'inégalité était inversée.

Jusqu'où faut- il aller pour mettre en évidence des x comme cela ? En d'autres termes, est-ce qu'on peut donner une borne supérieure, est-ce qu'on peut donner un majorant pour le premier x où l'inégalité est inversée ? Eh bien, oui ! On peut donner des majorants. Mais vous allez voir : ils sont grands.

Les premier majorants qui ont été proposés :

– Skewes 1933-1955, c'est le nombre $10^{10^{10^{10^3}}}$. Vous prenez 10 à la puissance 3, cela fait 1000 ; vous élevez 10 à la puissance 1000, vous élevez 10 à ce nombre-là, et vous élevez 10 à ce nombre-là. Ce sont des nombres inimaginables, absolument inimaginables, hors de toute réalité physique.

– Cela a été abaissé. À ma connaissance, le dernier majorant connu, c'est : $6,7.10^{370}$. Cela date d'il y a un peu plus de dix ans. Mais vous le voyez, aucun ordinateur ne peut aller jusque là.

Deux tout petits commentaires là-dessus :

– Ce nombre-là, il appartient à $\mathbf{N}$, l'ensemble des entiers naturels. Je doute qu'on puisse dire que c'est un entier « naturel ».

– Deuxième remarque : une bonne partie de la théorie des nombres vient de l'observation des nombres. Et dans les grandes étapes que je vais vous décrire toute de suite, l'observation a joué un rôle essentiel. Les ordinateurs nous permettent de multiplier les observations, d'avoir accès à des nombres que les meilleurs calculateurs du temps passé ne pouvaient pas aborder. Mais l'observation n'est pas seule. Par delà l'observation, il y a le raisonnement, il y a la méthode, il y a la démonstration mathématique. Et il peut arriver à la démonstration mathématique de contredire l'intuition résultant de l'observation.

Maintenant, suite de la promenade !

I retour en arrière

$$\pi(x) = \sum_{p<x} 1$$

Euclide, livre 9, prop. 10 $\to \infty$

Euler 1737 $\sum \frac{1}{p} = \infty$

Legendre 1808 $\simeq \frac{x}{\log x - a}$

Gauss $\sim$ 1808 ? $< li\, x$?

Riemann 1859 $\sum \frac{1}{n^s} = \zeta(s) = \prod(1-\frac{1}{p^s}$

Tchebycheff 1850 $a < \frac{\pi(x)}{x/\log x} < b$

Hadamard
de la Vallée Poussin 1896 $\pi(x) \sim \frac{x}{\log x} \; (\sim li\, x)$

Littlewood 1914

Erdös
Selberg 1949

Livres

Ingham 1932

Mendès-France et Tenenbaum 1997

Demazure 1997

Transparent II

Je rappelle la définition de $\pi(x)$: le nombre de nombres premiers inférieurs à x.

• Euclide, livre 9, proposition 10, avec un énoncé et une démonstration impeccable :

$\pi(x)$ tend vers l'infini quand x tend vers l'infini.

En réalité, Euclide dit beaucoup mieux. Il dit : quelle que soit la collection – il entend collection finie – de nombres premiers, je peux trouver un nombre premier en dehors de cette collection.

• Euler, 1737 : c'est la divergence de la série $\sum \frac{1}{p}$, p premier.

Bon, là c'est bien ! On va pouvoir réfléchir sans tableau. Comment est-ce qu'on démontre cela ? Songez que les produits infinis et les séries sont associés, et que, à la série $\sum \frac{1}{p}$ nous pouvons associer le produit infini $\prod \left(1 - \frac{1}{p}\right)$. Les deux vont converger ou diverger en même temps. Mais diverger pour un produit infini dont les produits partiels sont plus petits que 1, cela signifie tendre vers zéro. Donc cela signifie que $\prod \left(1 - \frac{1}{p}\right)^{-1}$ tend vers l'infini.

Mais est-ce que cela est vrai ? Oui, parce que si l'on développe $\left(1 - \frac{1}{p}\right)^{-1}$, on trouve : $1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots$, et quand on multiplie tous ces facteurs, qu'obtient-on ?
On obtient $\sum \frac{1}{n}$ portant sur tous les entiers.

Euler a donc, à partir de la divergence de la série des inverses des entiers, $\sum \frac{1}{n}$, démontré par ce procédé ingénieux, la divergence de la série des inverses des nombres premiers.

• Legendre, 1808, a cherché à approcher $\pi(x)$ par une expression de la forme $\frac{x}{\log(x)-a}$. Je vous ai montré tout à l'heure ce qui se passe avec $a = 1$, et $a = 1$ est la meilleure valeur quand on prend de très grandes valeurs de x, mais Legendre, qui n'en prenait pas de si grandes, avait pensé que $a = 1+$ « un petit quelque chose » était meilleur. C'était de l'expérimentation mathématique.

• Gauss quand il était jeune, avant 1800, a comparé $\pi(x)$ et $\mathrm{li}(x)$. Il s'est aperçu que c'était très proche et il a observé que $\pi(x)$ était inférieur à $\mathrm{li}(x)$. C'est resté comme la *conjecture de Gauss*. Mais Gauss n'a jamais écrit cette conjecture, il était bien trop prudent.

• Riemann, en 1859 : mettez $s = 1$ dans la formule que j'ai écrite ; vous obtenez exactement ce que je vous racontais tout à l'heure : $\zeta(1)$ c'est $\sum \frac{1}{n}$. Le second membre, c'est un produit infini qui s'appelle *le produit d'Euler*. $\zeta(s)$ admet deux expressions, et on peut jouer avec ces deux expressions, le produit fini : $\prod \left(1 - \frac{1}{p^s}\right)^{-1}$, et la série infinie : $\sum \frac{1}{n^s}$. Je vous dirai un mot de ce que Riemann a fait avec la fonction $\zeta(s)$ et de l'actualité des recherches en cours sur $\zeta(s)$.

• Tchebycheff, avant l'article de Riemann, avait démontré par des moyens qu'on appelle « élémentaires », ce qui ne signifie pas « faciles », que $\pi(x)$ était compris entre $\frac{ax}{\log x}$ et $\frac{bx}{\log x}$ avec des valeurs de a et de b, l'une inférieure à 1, et l'autre supérieure à 1, mais assez rapprochées pour que Tchebycheff ait été capable, à partir de là, de montrer qu'entre deux puissances de 2 consécutives, il existait toujours un nombre premier. C'était probable, vu la divergence de la série $\sum \frac{1}{p}$, mais la démonstration n'est pas facile.

• En 1896 – on a fêté la chose il y a deux ou trois ans –, ce fut la découverte, indépendamment par Hadamard et par de la Vallée Poussin, du grand théorème des nombres premiers : $\pi(x)$ est équivalent à $\frac{x}{\log x}$ qui lui même est équivalent, je vous l'ai dit tout à l'heure, à $\mathrm{li}(x)$. Et de la Vallée Poussin a un peu précisé les choses, d'où résulte la validité de l'inégalité que j'indiquais tout à l'heure. Cette inégalité résulte de l'estimation donnée par de la Vallée Poussin de $\pi(x) - \mathrm{li}(x)$.

Il faut dire qu'aussi bien les recherches de de la Vallée Poussin que celles d'Hadamard étaient fondées sur une exploration des propriétés de $\zeta(s)$ comme fonction d'une variable complexe qui avaient été initiées par Riemann,– cela avait été le grand travail de Riemann –, mais qui avaient été poursuivies aussi par Hadamard dans sa thèse qui était consacrée aux fonctions entières et à la comparaison entre leur ordre de croissance et la répartition de leurs zéros. J'évoque ici pour la première fois, j'y reviendrai, les zéros de la fonction $\zeta(s)$ de Riemann.

• Littlewood en 1914 : c'est ce que je vous ai raconté à l'instant, c'est que la seconde inégalité, évidente sur le tableau, est fausse.

• Erdös et Selberg, 1949. Cela a été une surprise dans le monde mathématique comparable à la surprise causée par la découverte de Hadamard et de la Vallée Poussin. Hadamard et de la Vallée Poussin, c'était la victoire de la théorie des fonctions, entendue comme théorie des fonctions d'une variable complexe, dans des domaines de la mathématique où on ne l'attendait pas : la théorie des nombres. Et pendant longtemps, on a pensé que le théorème des nombres premiers n'était accessible que par les méthodes qu'on appelait alors *transcendantes*, c'est-à-dire les méthodes utilisant la théorie des fonctions. On voyait bien que la méthode de Tchebycheff n'aboutirait jamais au théorème des nombres premiers, et on ne pensait pas que des méthodes élémentaires puissent suffire.
Alors en 1949, Erdös et Selberg – Selberg a eu la médaille Fields pour cela – ont obtenu une démonstration élémentaire du théorème des nombres premiers.

J'indique trois livres. Il y en a des multitudes sur les nombres premiers !

– Le livre d'Ingham, 1932, dont il y a eu une réédition, avec une préface merveilleuse, il y a quelques années. Il a été la Bible, je crois, sur les nombres premiers pendant longtemps ! C'est un petit livre dans les Cambridge Tracts in Mathematics. Mais c'est un livre, en anglais, absolument superbe.
Ingham croyait qu'il n'y aurait jamais de démonstration élémentaire du théorème des nombres premiers.

– Mendès-France et Tenenbaum : c'est le plus récent des livres sur les nombres premiers. Il a l'intérêt d'être un livre de poche, dans la collection des Presses Universitaires de France. C'est un *Que sais-je ?*, un *Que sais-je ?*, je dois dire, assez difficile. Il vient d'obtenir lundi dernier [29/3] le prix de la vulgarisation scientifique de l'Académie des Sciences. Je pense qu'au point de vue scientifique c'est parfaitement justifié. Au point de vue de l'accessibilité à un large public, je vous invite à en juger par vous-mêmes.

– Demazure, 1997. Cela s'appelle *Cours d'Algèbre*. C'est édité par un nouvel éditeur, Cassini, et pour moi c'est assez fascinant ! On a parlé tout à l'heure – M. le Recteur, d'abord – de l'influence qu'avait l'informatique sur le développement des mathématiques. Eh bien, si vous regardez le livre de Demazure, vous en avez une preuve vivante ! Il aborde des questions qui sont des questions classiques d'Algèbre, et aussi bien des questions très modernes, mais à partir des préoccupations qu'il suppose chez ses élèves de l'École polytechnique, et qui reposent largement sur l'utilisation de l'informatique dans des domaines que je vais indiquer tout de suite.

Tout de suite, c'est l'autre transparent : *En avant !* C'est pour que vous ne restiez pas sur l'impression que les nombres premiers c'est de l'histoire.

I en avant !

Quelques problèmes

historiques

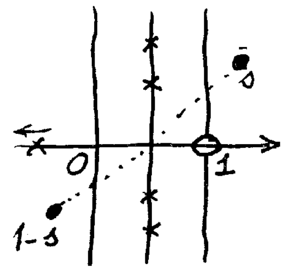
Goldbach $\qquad$ pair $= p + p'$

Nombres premiers jumeaux $\quad p, p+2$

$\pi(x) - \mathrm{li}\, x = O(x^a)$ quand $a > \frac{1}{2}$

$\Updownarrow$

hypothèse de Riemann : les zéros de $\zeta(s)$ situés dans la "bande critique" $0 < \sigma < 1$ sont sur la droite $\sigma = \frac{1}{2}$.



$s = \sigma + it$

actuels

$a^p \equiv a \pmod p$ $\qquad$ relations à l'algèbre et aux probabilités (tests de primalité)

$P \quad NP$ $\qquad$ à la cryptographie et à la logique (décomposition en facteurs premiers)

à la physique (distribution des zéros sur $\sigma = \frac{1}{2}$)

à l'informatique

Exercice.

Caractériser les nombres premiers qui sont sommes de deux carrés.

$$p = a^2 + b^2 = (a+ib)(a-ib) \qquad \mathbb{Z} + i\mathbb{Z}$$

Transparent III

Problèmes historiques

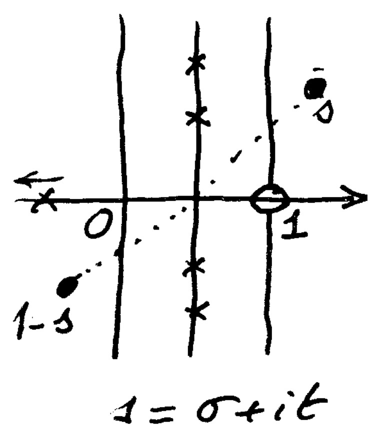
D'abord, l'histoire nous a légué des problèmes qui sont, parmi les problèmes non résolus les plus fascinants pour des mathématiciens : les grands problèmes historiques.

• Goldbach, milieu du XVIII^{e} siècle : est-ce que tout nombre pair est la somme de deux nombres premiers ? Je ne vous fais pas le point sur les résultats partiels. On sait maintenant que tout nombre impair assez grand est la somme de trois nombres premiers : cela, c'est Vinogradov, avant la guerre. On sait que tout nombre pair est la somme d'un nombre premier et d'un produit de deux nombres premiers : c'est un chinois, Chen, assez récemment. Mais le problème de Goldbach reste un problème apparemment très difficile. Il sera résolu, mais... je ne sais pas quand !

• Nombres premier jumeaux : c'est également un problème qui sera résolu. Le résultat est clair : il existe une infinité de nombres premiers jumeaux, tels que 3 et 5, 11 et 13, 29 et 31 etc. On a maintenant une foule d'arguments convaincants pour être moralement sûr qu'il existe une infinité de couples de nombres premiers jumeaux. Mais la démonstration risque de tarder encore. C'est un problème apparemment très difficile.

• Et puis il y a l'estimation de $\pi(x) - \mathrm{li}(x)$. Je vous ai dit que la première estimation, c'était de la Vallée Poussin. On en est à l'heure actuelle à des estimations où $\pi(x) - \mathrm{li}(x)$ est estimé comme petit par rapport à $xe^{(-a\sqrt{\log x})}$. On ne va pas beaucoup plus loin. Et la grande hypothèse, c'est que $\pi(x) - \mathrm{li}(x)$ est compris entre x^a et $-x^a$ lorsque a est supérieur à $\frac{1}{2}$, pour x assez grand. Cet énoncé est équivalent à l'hypothèse de Riemann qui est maintenant, sans doute, l'hypothèse la plus fameuse chez les mathématiciens : que les zéros de la fonction $\zeta(s)$ qui sont situés dans la bande partie réelle de s entre 0 et 1 se trouvent tous sur la droite $\sigma = \frac{1}{2}$.

Comme je viens de l'indiquer ici, les zéros doivent être sur cette droite-là. Il y a, à vrai dire, des zéros sur l'axe réel négatif. Tous les entiers négatifs pairs sont des zéros de la fonction $\zeta(s)$ de Riemann. La fonction $\zeta(s)$, Riemann avait montré qu'elle avait une propriété extraordinaire : c'est une fonction méromorphe. Elle a un seul pôle au point 1. Cela veut dire : $(s-1)\zeta(s)$ est une fonction entière. Et puis, de la connaissance de $\zeta(s)$ en un point, on tire, par une formule qui s'appelle l'*équation fonctionnelle de Riemann*, la valeur de $\zeta(s)$ au point symétrique par rapport au point $\frac{1}{2}$, c'est-à-dire le point $1-s$. Donc cette droite-là [$\sigma = \frac{1}{2}$] joue un rôle de symétrie dans la théorie de la fonction $\zeta(s)$ de Riemann.



Ça, ce sont des problèmes historiques. Passons aux problèmes actuels.

Problèmes actuels

• *Relations à l'algèbre et aux probabilités* : reconnaître si un nombre est premier.

Les spécialistes nous disent maintenant que ce problème est résolu. Allez voir Demazure pour comprendre dans quel sens il est résolu. Il est résolu parce que, en se fondant sur des théorèmes d'algèbre, du type du vrai théorème de Fermat, le théorème $a^p = a$ modulo p, quand p est premier, – naturellement, ce n'est pas vrai quand p n'est pas premier –, eh bien, rien que ce théorème-là constitue un test de primalité, parce que si cela n'est pas vrai pour un certain p, c'est que p n'est pas premier. Les tests de primalité actuels sont assez surprenants. On décide qu'un nombre très grand est premier avec une très grande probabilité ; pour toutes les applications qu'on souhaite, et en particulier les applications à la cryptographie, c'est suffisant. Je ne vous détaille pas la chose. Encore une fois, je vous renvoie à Demazure si ça vous intéresse. Il y a quelques mots là-dessus, d'ailleurs, dans Mendès-France et Tenenbaum.

• *Relations à la logique*
Il s'avère que découvrir si un nombre est premier, c'est considéré maintenant comme un problème « résolu ». Mais factoriser un nombre dont on sait qu'il est le produit de deux facteurs premiers – très grands –, ça, c'est un problème qui n'est pas résolu ! Et, pour le moment, il est inabordable. C'est, pour le moment, le candidat à être un problème de la classe NP. Les logiciens et les informaticiens distinguent les problèmes de la classe P : les problèmes abordables, et les problèmes NP : les problèmes non abordables ; et un candidat à être un problème non abordable, c'est la décomposition en facteurs premiers. Ces recherches présentent un intérêt en cryptographie à ce point que, en 1985, les services de sécurité américains avaient décidé de contrôler toutes les publications sur la divisibilité des nombres entiers, et avaient demandé à la Société Américaine de Mathématiques de concourir avec eux pour soumettre à leur examen préalable tout ce qui devait se publier sur le sujet. Il y a eu une réaction très vigoureuse de la Société Américaine de Mathématique, parce qu'ils sont bien organisés aussi là-bas, et les services de sécurité américains ont dû reculer.

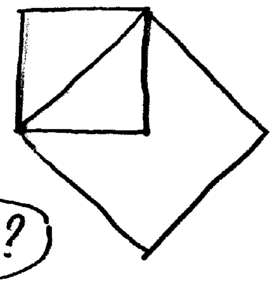
• *Applications et liens à la physique*
J'ai reçu juste avant de partir le numéro de Janvier du bulletin de la Société Américaine de Mathématique. Le grand article de « survey », – grand article d'exposition –, c'est un article qui s'appelle *zéros de la fonction $\zeta(s)$ et symétries*, et les symétries sont entendues au sens des physiciens. Il se trouve que la relation entre les zéros de la fonction $\zeta(s)$ et les valeurs propres de certaines matrices aléatoires a été mise en évidence par les physiciens, à savoir par Wigner et ses continuateurs avant de pouvoir être abordée par des mathématiciens.
Donc, c'est à la fois relations à la physique et aux probabilités.

• Comme je viens de parler de choses très savantes, je voudrais revenir à un exercice, un exercice pour nos élèves. Je l'ai pratiqué avec un club mathématique au lycée Condorcet, dans les années 1960. Cela s'était passé à 15 jours d'intervalle. Faire une table des nombres premiers. Regarder parmi ces nombres premiers ceux qui sont somme de deux carrés, c'est le cas pour 5 : 1+ 4, et ceux qui ne le sont pas comme 7. Quels sont les nombres premiers qui sont somme de deux carrés et ceux qui ne sont pas somme de deux carrés, et essayer de découvrir une loi.
Comme on n'a pas le temps de faire l'exercice, il faut, à mon grand regret, vous donner la réponse, pour ceux d'entre vous qui ne la connaissent pas. Les nombres premiers qui sont décomposables en somme de deux carrés ce sont les nombres premiers qui sont égaux à 1 modulo 4. Ceux qui ne sont pas décomposables sont ceux qui sont égaux à 3 modulo 4. La seconde assertion est très facile à vérifier. En effet un carré est toujours égal à 0 ou 1 modulo 4. Je vous donne le temps de réfléchir. La réflexion est faite ? D'accord.
Donc tout carré est égal à 0 ou 1 modulo 4. Quand vous ajoutez 0 ou 1 à 0 ou 1, ça ne va jamais vous donner 3. Par conséquent, les nombres qui sont 3 modulo 4 ne sont pas sommes de deux carrés, qu'ils soient premiers, ou pas premiers.
Maintenant, nombres premiers sommes de deux carrés. Fermat avait découvert la loi, mais c'est Gauss qui a fait la bonne démonstration.
Après l'expérimentation faite par les élèves, j'ai entrepris cela, et c'était un peu audacieux. C'étaient des élèves de Seconde, donc ils ne connaissaient pas les nombres complexes. Et pourtant la décomposition en somme de deux carrés se comprend bien si on écrit $p = a^2 + b^2$, cela signifie $p = (a+ib)(a-ib)$; c'est-à-dire que p, qui est premier sur les entiers, se décompose en un produit de facteurs sur l'anneau des entiers de Gauss $\mathbf{Z}+i\mathbf{Z}$. Et, effectivement, Gauss a démontré le théorème que je vous ai dit dans ses

Recherches arithmétiques qui datent de sa jeunesse et où il a introduit l'anneau des entiers de Gauss.
Donc, c'est un exercice qui est d'abord une expérimentation, et ensuite un essai de démonstration.
Je termine là la PROMENADE I. La PROMENADE II va être une promenade à travers les irrationnels.

Promenade II

à travers les irrationnels.

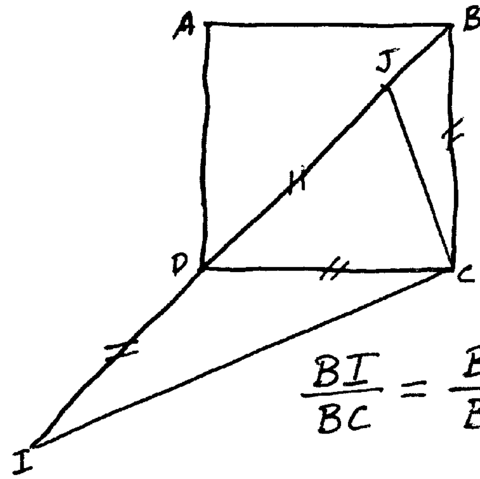


Platon et $\sqrt{2}$

Théétète et Théodore

$\sqrt{2}, \ldots\ldots, \sqrt{17}$ $\quad$ $\sqrt{19}\,?$

Une interprétation



$$1+\sqrt{2} = 2 + \cfrac{1}{1+\sqrt{2}}$$

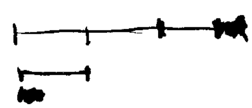
$$= 2 + \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cdots}}}$$

$$= (2, 2, 2, 2, \cdots)$$

$$\frac{BI}{BC} = \frac{BC}{BJ}$$

$$\frac{1+\sqrt{5}}{2} = (1, 1, 1, 1, \cdots)$$

$$\frac{3+\sqrt{13}}{2} = (3, 3, 3, 3, \cdots)$$



$$1+\sqrt{3} = (2, 1, 2, 1, \cdots)$$

$n =$	2	3	5	6	7	10	11	13	14	15	17	19
κ) =	2,4	3,7	1,6	9,9	16	6,1	20	3,3	30	7,8	8,1	340

$$p^2 = 2q^2$$

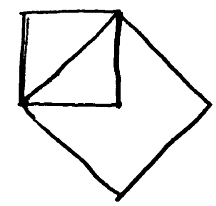
Transparent IV

PROMENADE II : A travers les irrationnels

J'aimerais bien m'attarder et vous raconter des histoires, mais il est déjà un petit peu tard. Tant pis !

Platon et $\sqrt{2}$

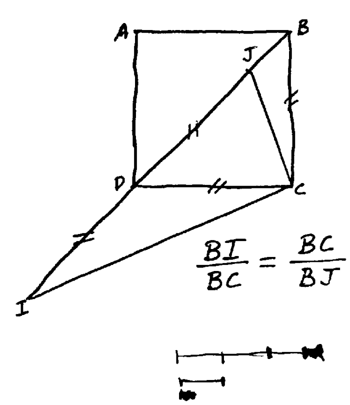
Platon a été toujours fasciné par la duplication du carré ; cf. la leçon de Socrate à l'esclave de Ménon, où Socrate enseigne à cet esclave, prétendument en utilisant la méthode maïeutique, comment doubler un carré.
Pour doubler un carré, il ne faut pas doubler le côté, il ne faut même pas multiplier le côté par $\frac{3}{2}$, il faut prendre la diagonale. Bon, eh bien, j'ai fait le dessin. Il apparaît au terme de la leçon de Socrate à l'esclave de Ménon.



Mais Platon a été fasciné par une autre chose. Il a su – quand ? je ne sais pas – que $\sqrt{2}$ était irrationnel, non exprimable comme une fraction. Et pour lui, ce n'est pas cela qui était la chose étonnante. Elle était plus ou moins de connaissance commune depuis plus d'un siècle. Non, la chose vraiment étonnante c'était l'interprétation. C'était que deux carrés puissent être commensurables en surface à savoir l'un double de l'autre, sans être commensurables en longueur, à savoir que le rapport des côtés était un nombre irrationnel. Là, je me réfère à un souvenir. Ce doit être dans *Les Lois*, où n'apparaît pas Socrate, où il apparaît l'Athénien – l'Athénien a une quarantaine d'années, et c'est vraisemblablement Platon – ; l'Athénien dit que lorsqu'il a découvert cela et qu'il s'est aperçu que c'était largement ignoré de tous les Grecs, il lui a semblé que les Grecs ne valaient pas mieux que des *pourceaux à l'engrais* !
Platon est revenu sur l'irrationalité dans un dialogue où il met en scène un jeune mathématicien : Théétète. Je vous conseille la lecture des premières pages du *Théétète*.

Théétète est un jeune homme, il est très laid, aussi laid que Socrate. Il a moins de 20 ans, il va mourir à la guerre du Péloponnèse. Les historiens hésitent : seconde guerre du Péloponnèse, il aurait 40 ans, première guerre du Péloponnèse, il aurait 20 ans. Pour moi, il n'y a absolument aucun doute, il est mort à la première guerre du Péloponnèse. Il n'a laissé aucune œuvre écrite, mais une réputation étonnante, dont justement le dialogue de *Théétète* se fait l'écho.
Socrate demande à Théétète ce qu'il a appris et ce qu'il a fait. Eh bien, il a appris de son maître Théodore l'irrationalité de $\sqrt{2}$, $\sqrt{3}$, – je saute quand même $\sqrt{4}$! –, $\sqrt{5}$, jusqu'à $\sqrt{17}$. Et, *pour une certaine raison*, Théodore s'est arrêté là. Le terme utilisé par Platon c'est que Théodore a *montré* cela à Théétète. Mais peut-être l'a-t-il montré sur des figures ? Et les commentateurs ne sont pas tous d'accord sur ce point.

Mon interprétation, celle que je vais vous soumettre, est qu'il l'a montré sur des figures.
Ne regardez pas ce qu'il y a à gauche [transparent IV], regardez ce qu'il y a à droite : à droite, il y a le carré, il y a la diagonale, et maintenant, on va essayer de mesurer la diagonale à partir du côté.
Vous savez qu'il y a l'algorithme d'Euclide pour la comparaison des longueurs :
Quand on a deux longueurs à comparer, eh bien, on prend la plus grande, on porte la plus petite dans la plus grande autant de fois qu'on le peut. Si le reste est nul, eh bien, c'est parfait ! On a découvert que la plus grande est un multiple de la plus petite ; et puis sinon, eh bien on recommence en faisant jouer à la plus petite le rôle de la plus grande, et au reste, le rôle de la plus petite. C'est cela l'algorithme d'Euclide.



Alors, appliquons l'algorithme d'Euclide. Eh bien, on porte dans la diagonale sous la forme DJ un segment – on ne peut pas en porter deux ! – égal au côté DC. Pour faire bonne mesure et avoir une belle figure, on va porter DI symétrique de DJ, par rapport à D, c'est-à-dire qu'on va mesurer, si vous voulez : *côté plus diagonale par rapport au côté*.

Si je prends côté plus diagonale, je porte deux fois le côté, puis j'ai un reste. Le reste, c'est JB. JB doit maintenant me servir à mesurer la petite longueur qui est BC. Alors JB mesure BC, exactement de la même façon que BC mesure BI. Les géomètres sont très bons en géométrie... et savent que ces triangles [BIC et BJC] sont semblables. Cela veut dire que si je continue avec le petit triangle ce que j'ai commencé avec le grand, j'obtiendrai un nouveau petit triangle qui sera semblable aux précédents, et j'obtiendrai une suite de triangles emboîtés, toujours semblables les uns aux autres, sans que jamais cela ne s'arrête. Si l'algorithme d'Euclide ne s'arrête pas, c'est que les quantités sont incommensurables.

Je pense que cela pouvait être la démonstration de Théodore, et je vais le traduire maintenant en termes de calculs tout simples.

$1+\sqrt{2}$, c'est $2+(1$ divisé par $1+\sqrt{2})$. C'est exactement la traduction de ce que je viens de dire. BC mesuré par JB, c'est $1+\sqrt{2}$. C'est la même chose que BI mesuré par BC, c'est-à-dire $1+\sqrt{2}$. Mais alors, le $1+\sqrt{2}$ qui est ici, je peux l'écrire à son tour sous la forme $2+\frac{1}{1+\sqrt{2}}$, et je peux continuer comme cela : ça ne va jamais s'arrêter !

$$1+\sqrt{2} = 2+\frac{1}{1+\sqrt{2}} = 2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cdots}}} = (2,2,2,2,\dots)$$

$$\frac{1+\sqrt{5}}{2} = (1,1,1,1,\dots)$$

$$\frac{3+\sqrt{13}}{2} = (3,3,3,3,\dots)$$

Cela forme ce qu'on appelle une fraction continue. La notation abrégée, est (2, 2, 2, 2, ...). Alors, la méthode de Théodore exprimée en termes actuels, cela a pu être de découvrir des fractions continues – naturellement, il n'avait pas le terme – qui correspondent à des nombres liés à $\sqrt{3}$, $\sqrt{5}$, etc. jusqu'à $\sqrt{17}$ et traduire un développement simple en fraction continue sous la forme d'un argument géométrique de répétition par ce qu'on appellerait maintenant *autosimilarité*.

Et je pense que ce peut être le cas parce que, effectivement, regardez :

$\frac{1+\sqrt{5}}{2}$, c'est (1, 1, 1, 1, ...) : l'argument géométrique sera très facile à produire.

$\frac{3+\sqrt{13}}{3}$, c'est (3, 3, 3, 3, ...) : l'argument géométrique sera facile à produire.

Par contre, pour $\sqrt{3}$, il n'y aura pas de facteur périodique avec un seul terme. $1+\sqrt{3}$, ce sera (2, 1, 2, 1, 2, 1, ...). Mais la répétition même du motif 2, 1 fait que non pas en une étape, mais en deux, on arrivera à des triangles semblables. Deux correspond au fait qu'il y a ici une période 2, et on arrivera à des triangles semblables avec des rapports de similitude.

Ces rapports de similitude, je les ai calculés pour les nombres jusqu'à $\sqrt{17}$. Ils ne sont pas très grands. Et puis, pour $\sqrt{19}$, le rapport de similitude absolument nécessaire si on veut utiliser cet argument que je prête à Théodore, il « explose ». Alors, voilà les nombres :

$n =$	2	3	5	6	7	10	11	13	14	15	17	19
$k) =$	2,4	3,7	1,6	9,9	16	6,1	20	3,3	30	7,8	8,1	340

Pour $n = 2, 3$, etc., j'ai ôté les nombres qui contenaient en facteur un carré, je n'ai conservé que les nombres que les Allemands appellent « quadratfrei ». Eh bien, jusqu'à $\sqrt{17}$, voyez : le « pire » des nombres c'est 14 pour lequel ce rapport de similitude est voisin de 30, mais pour 19, il saute à 340. Donc la figure est impossible à faire. Les autres figures, je les ai faites à la main, ça marche.

Problème de la démonstration de $p^2 = 2q^2$

Bon, alors maintenant, vous connaissez tous la démonstration d'Euclide pour l'irrationalité de $\sqrt{2}$. Si $\sqrt{2}$ était égal à $\frac{p}{q}$, on aurait $p^2 = 2q^2$. Et cela veut dire que p serait pair, mais si p est pair, c'est aussi que q est pair, et donc que la fraction n'est pas irréductible. Et si on la suppose irréductible au départ, il y a contradiction.

Vous pouvez aussi montrer l'impossibilité de cela en calculant modulo 3 : modulo 3, p^2 c'est ce que j'ai dit tout à l'heure, $2q^2$; vous ne pouvez avoir égalité que si p et q sont multiples de 3. Vous pouvez varier les arguments ; que ce soit l'argument d'Euclide ou un argument modulo « quelque chose », ces arguments se prêtent parfaitement à l'étude de $\sqrt{19}$. Il n'y a pas de différence entre $\sqrt{2}$ et $\sqrt{19}$ pour l'approche d'Euclide.

Euclide c'est un petit siècle après Théétète : mon hypothèse, je crois que c'est l'hypothèse générale, c'est que la démonstration d'Euclide est la démonstration trouvée par Théétète. Théétète a une méthode générale : c'est ce qui résulte de la lecture de Platon. Platon n'a pas été capable d'exposer cette méthode générale, sans doute, il ne l'aurait pas comprise d'ailleurs, mais il dit qu'il y a une méthode générale, donc c'est sans doute le fait de Théétète. Et Théétète, c'est aussi, à ma connaissance, la première introduction explicite d'un raisonnement par l'absurde.
Donc, le mérite de Théétète dans l'histoire des mathématiques me paraît éclatant, mais cela n'exclut nullement qu'il soit mort à l'âge de 20 ans !

Bon, il ne faut pas que je vous raconte trop d'histoires sur Théétète, parce que je voudrais quand même qu'on fasse un tout petit peu de mathématiques. Alors : jouer avec les fractions continues.

II Jouer avec les fractions continues

a) $\dfrac{a+b\sqrt{c}}{d} \longrightarrow$ période

b) $e^{1/n} \longrightarrow$ loi simple

$n=1 \qquad (2,1,\underline{2},1,1,\underline{4},1,1,\underline{6},1,\dots)$

$n=2 \qquad (1,\underline{1},1,1,\underline{5},1,1,\underline{9},1,1,\underline{13},1\dots$

c) $\pi \qquad (3,7,15,1,293,\dots)$

$\longrightarrow$ bonnes approximations $\dfrac{22}{7}, \dfrac{355}{113}$

$\pi^4 \qquad (97,2,2,3,1,17089,\dots)$

$\longrightarrow$ excellente approximation $\dfrac{2143}{22}$

d) Ex : $\dfrac{787}{522} = 1{,}507662835$

Comment remonter ?

Transparent V

Jouer avec les fractions continues

J'ai apporté ici ma « Sharp ». C'est un truc qu'on met dans la poche, dans lequel j'ai mis des programmes pour jouer avec les fractions continues. Et naturellement, si vous me proposiez de jouer, je vous montrerais que je peux jouer, et très vite : j'ai bien programmé !

a) Alors les nombres. D'abord, je vais employer un « gros mot » : les nombres des corps quadratiques réels. Cela signifie tout simplement les nombres qui sont de la forme $\frac{a+b\sqrt{c}}{d}$, où a, b, c d sont des nombres entiers positifs. Eh bien, tous ces nombres-là, lorsqu'on les développe en fractions continues, il y a un début dont je ne peux rien dire, et puis, à partir d'un certain moment, hop là !, ça devient périodique, comme j'ai vu une période apparaître pour $1+\sqrt{2}$.
Alors on peut varier les exercices ; on peut vérifier que, pour chaque valeur de c, en tâtonnant on arrivera à trouver a, b et d de telle manière que la période soit 2. Cela, c'est un petit théorème que vous pouvez découvrir par expérimentation.

b) En dehors des nombres des corps quadratiques réels, on peut faire l'expérimentation, si on est ignorant comme moi je l'étais à l'époque : on tape e, et puis on regarde ce que cela donne.
Alors, quand on voit e, cela donne 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, ... Tiens ! Peut-être est-ce qu'après il y aurait 1, 8, 1 ? Eh bien justement, après il y a 1, 8, 1. Peut-être est-ce qu'après il y aurait 1, 10, 1 ? Oui, après il y a 1, 10, 1. Peut-être est-ce qu'après il y a 1, 12, 1 ? Ah, non ! Après, il y a 2, 90, 12, parce que, naturellement, à partir d'un certain moment, la calculette fait des fautes. La calculette est un moyen de découvrir, pas un moyen de démontrer.
Justement, ce n'est pas si mauvais de faire découvrir, et après de démontrer. Alors je dois dire que démontrer pour les corps quadratiques réels qu'ils ont une période, ce n'est pas trop difficile. Pour e, je me suis cassé la tête, enfin... je l'ai fait quand même ! C'est une connaissance classique qu'il y a cette espèce de semi-périodicité pour e et en général pour les nombre de la forme $e^{1/n}$, mais enfin, si vous voulez le chercher tout seuls, faites cela pendant les vacances ! Ensuite, il y a des nombres qui n'ont aucune régularité décelable dans le développement en fractions continues.

c) Le nombre π n'a aucune régularité décelable. Mais si j'écris ici les premiers termes (3, 7, 15, 1, 293, ...), c'est parce qu'il apparaît quelque part un 293. C'est assez grand, 293 , $\frac{1}{293}$ c'est petit. Donc quand vous écrivez la fraction continue et que vous avez plus quelque chose, vous ne ferez peut-être pas une très grande faute en remplaçant cela par 0. Alors, lorsqu'on remplace $\frac{1}{15}$ par 0, on obtient la bonne approximation $\frac{22}{7}$. Lorsqu'on remplace $\frac{1}{293}$ par 0, on obtient la bien meilleure approximation $\frac{355}{113}$.
Règle. Vous faites avec votre calculette le programme le plus « minable » possible : entrez x, affichez partie entière de x, prenez l'inverse de x – partie entière de x, répétez. C'est tout. Et après cela, vous cliquez, vous cliquez, vous cliquez..., et vous obtenez ce qu'on appelle les quotients incomplets, c'est-à-dire les nombres entiers qui apparaissent dans le développement en fractions continues. Quand vous tombez sur un grand nombre, vous savez qu'il faut vous arrêter juste avant, que vous avez acquis une bonne approximation rationnelle.

Le plus amusant, c'est avec π^4 qui m'a été révélé par un physicien. Alors, π^4 : 97, 2, 2, 3, 1, rien d'extraordinaire. Puis 17089 : là, c'est vraiment le candidat à être l'infini ! Cela donne une excellente approximation qui est : $\frac{2143}{22}$.
Là, voilà ! Si on avait le temps on ferait des exercices. Je vous signale un exercice, mais on manque de temps.

d) Exercice : $\frac{787}{522} = 1,507662835$. Comment remonter ?
Je prends la calculette et, en mode « calcul », je calcule, non, je vous fais calculer . Alors, vous obtenez un nombre. Combien a-t-il de chiffres ?... Il a 10 chiffres : vous obtenez un nombre à 10 chiffres ; vous

me dictez ces 10 chiffres. Je passe en mode « run », j'affiche ces 10 chiffres. J'exécute mon programme. Ma machine « réfléchit » pendant 3 secondes, et elle affiche $\frac{787}{522}$. Là il lui a fallu la petite théorie de récurrence sur les réduites des fractions continues. Ce n'est pas très difficile à programmer, mais dans une classe, je l'ai expérimenté, c'est assez spectaculaire !

D'ailleurs, dans les classes, ce peut être assez spectaculaire de faire des exercices beaucoup plus modestes. C'est pour les inspecteurs, peut être pas pour les inspecteurs pédagogiques régionaux, peut-être plus pour les inspecteurs de l'Éducation Nationale. Vous réunissez des professeurs d'École ou des instituteurs, et puis vous demandez à l'un d'entre eux :

- Est-ce que vous vous souvenez combien il y a d'élèves dans votre classe, combien il y a de filles ? Vous voulez prendre votre calculette, et me dire la proportion de filles. Vous me donnez simplement 3 chiffres significatifs.

- Oui : il y en a ... 51,5%.

- Ah bon ! Alors, vous avez une classe de... 33 élèves, avec 17 filles ! Il n'y a pas besoin là de calculette. Il suffit simplement de vous être fait une table de division. Au lieu de faire une table de multiplication, vous faites une table de division, vous consultez la table de division et vous regardez.

Alors, la table de division, je l'ai toujours sur moi, à toutes fins utiles... Mais on ne va pas l'utiliser aujourd'hui.

II Les fractions continues à travers l'histoire

a) ~ algorithme d'Euclide de comparaison des longueurs

b) fractions "babyloniennes" $a + \frac{1}{b}$

c) Laplace $\frac{22}{21}$ $\frac{25}{24}$

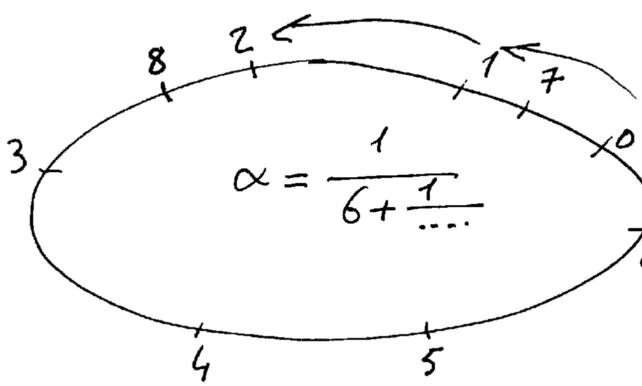
$1{,}047\ldots$ $1{,}041\ldots$

d) Legendre et le calendrier $365 + \frac{1}{4} \ldots$

e) Poincaré ...... Yoccoz

les homéomorphismes du cercle

et leur "nombre de rotation"



Transparent VI

Les fractions continues à travers l'histoire

Les fractions continues **à travers l'histoire**, parce que, naturellement, ce que je vous ai raconté de Théodore, c'est une fiction. Théodore n'avait pas la théorie des fractions continues, n'avait pas la pratique des fractions continues, peut-être une vague intuition fondée sur la similarité des objets géométriques.

a) Une première approche des fractions continues, c'est ce que je vous ai dit tout à l'heure : c'est l'algorithme d'Euclide de comparaison de longueurs.

Quand vous prenez la grande longueur que vous comparez à la petite, alors la première approximation du rapport, c'est un nombre entier qui est le nombre de fois que vous avez porté la petite dans la grande. Et puis, si vous répétez l'opération, une seule fois, vous obtenez une seconde approximation. Au lieu de la première approximation sous forme d'un nombre entier, vous obtenez l'approximation sous la forme d'un nombre entier plus l'inverse d'un nombre entier. Ce sont là les fractions qu'on a appelé *les fractions babyloniennes*.

b) Les fractions « babyloniennes » : $a+\frac{1}{b}$. Je n'ai pas trouvé trace de cela chez les babyloniens, mais j'espère que c'est vrai. Et en tout cas, les fractions babyloniennes étaient d'usage courant jusqu'au début du XIX^{e} siècle.

c) Laplace - autre histoire que je ne vous raconterai pas - compare le nombre de garçons à la naissance et le nombre de filles à la naissance. Il ne dit pas que la proportion est de $1,047$, il dit que la proportion est $\frac{22}{21}$. Il dit qu'il y a une anomalie à Paris, à savoir un peu moins de garçons par rapport aux filles ; il ne dit pas que la proportion est $1,041$, ce qui n'est pas tellement loin de $1,047$, il dit que la proportion est de $\frac{25}{24}$. Vous voyez, ce sont des *fractions babyloniennes*.

d) Legendre et le calendrier

Encore une fraction babylonienne, l'introduction des années bissextiles ! Quand on dit que l'année c'est 365 jours $+\frac{1}{4}$, c'est une *fraction babylonienne*.

Aussi bien, le premier exposé très nourri sur les fractions continues que je connaisse est le traité de Legendre où il commence par le calendrier.

Mais là, si l'on veut plonger dans l'actualité, on peut dire : les fractions continues sont, à l'heure actuelle, un outil essentiel pour les études sur les systèmes dynamiques.

e) Poincaré ... Yoccoz

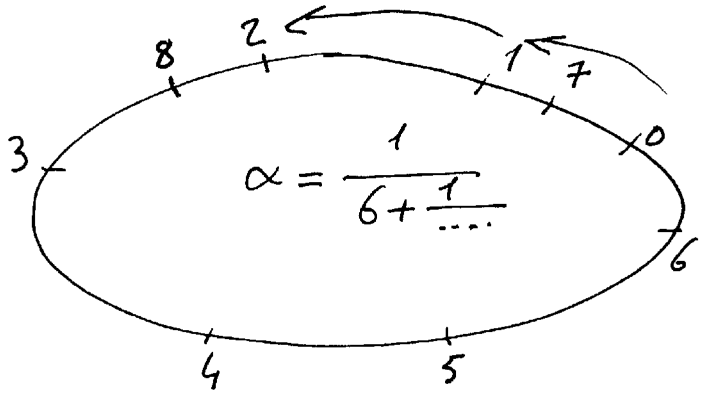
Les études sur les systèmes dynamiques, où les Français se sont particulièrement illustrés puisqu'on retrouve les noms de Denjoy, de Herman et maintenant de Yoccoz, remontent à Poincaré.

L'approche de Poincaré, c'était de réduire un mouvement, une trajectoire sur une surface par exemple, à l'itération d'une transformation sur un cercle. Sa méthode, c'était *la méthode des sections*.

Imaginez qu'on ait un tore, et qu'on ait une orbite, un mouvement sur le tore. Si vous faites une section du tore, par exemple par un méridien, alors, à ce moment-là, vous allez obtenir une suite de points.

Poincaré l'a appelée l'*orbite*, mais cela va être l'orbite d'une transformation qui sera la transformation qui ira du premier point d'intersection au deuxième point d'intersection. Et c'est la même transformation qui va du deuxième point d'intersection au troisième point d'intersection.

Et c'est la raison pour laquelle Poincaré s'est soucié d'une notion topologique. On prend un cercle topologique, qu'on peut dessiner n'importe comment, parce que cela veut dire un cercle que je peux déformer élastiquement comme je l'entends. Je peux lui donner la forme d'une patate, comme je l'ai fait ici.



Et puis on prend une transformation du cercle sur lui-même : c'est la transformation qui amène 0 sur le point 1, c'est la même transformation qui amène le point 1 sur le point 2, etc.
On regarde les orbites de cette transformation. Ici, après le point 6, vous passez au point 7 qui se retrouve entre 0 et 1. Cela veut dire que le premier nombre que vous allez écrire va être le 6. Le second nombre que vous aller écrire va résulter de la manière dont les points suivants vont se comporter par rapport à l'intervalle [0, 1].
Je ne vais pas continuer le dessin, mais vous obtenez comme cela une suite de nombres qui vont définir une fraction continue, et la fraction continue définit un nombre positif que Poincaré appelle *le nombre de rotation*.
Le nombre de rotation, si la transformation était une rotation sur le cercle, ce serait simplement l'angle de rotation sur le cercle. Si la transformation n'est pas une rotation sur le cercle, c'est la rotation qui est candidate à imiter cette transformation. Et la façon dont s'opère l'imitation a été l'objet des grandes recherches de Denjoy, de Yoccoz ; et c'est là que théorie de la mesure, et théorie des nombres en particulier, et théorie des fractions continues interfèrent.

Alors ? ... La dernière feuille, c'est ce que je vous ai annoncé : REPOS.

⋆

Repos.

→ 2 promenades dans une jungle.

π Delahaye transcendance, complexité

$a^n + b^n = c^n$ Fermat Kummer - idéaux Wiles < analyse, géométrie algébrique

Th des n. et analyse harmonique Wiener Vinogradov Weil

Groupes finis $\mathbb{N}$ $\mathbb{Z}$ $\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$ quaternions octavions

Cantor cardinaux, ordinaux transfinis

Arithmétique non standard

[Livres : cours d'arithmétique Serre JP

→ l'aventure des nombres Godefroy G.

le fascinant nombre π Delahaye J Paul]

→ Les nombres se racontent et s'écrivent

chanter les tables, comptines

Il était une fois, les 7 petits nains, les 3 petits cochons

contar - contar

zählen - erzählen

Babylone, archives 3200 tablettes cunéiformes

Chine Shang 1700 système décimal

Grèce Socrate Hippias – Arithmétique ordinaire

Indiens, Arabes, syst décimal et num. de position

Imprimerie, Neper, Stevin

Informatique

grands nombres, puissances de 10

~~femto~~ ~~pico~~ pico nano micro milli kilo méga giga tera | chang^t d'échelles milli - - kilo

10^{-12} -9 -6 -3 3 6 9 12

(→) Les nombres représentent autant qu'ils mesurent

températures

ascenseurs

$\bar{m}$ durée (big bang)

la droite numérique toujours plus intuitive (cf. Carnot)

complexes : varier les représentations et les usages

calcul modulo x^2+1

plan d'Argand

électricité.

→ Qu'est-ce qui est complexe, réel, naturel ?

Traces de l'histoire. Trompeurs | imaginaire, irrationnel, transcendant, idéal | et plus encore naturel

[Dehaene la bosse des maths

Animaux, enfants. Incroyable construction humaine (+1 → ∞)

Que notre enseignement donne aux enfants et aux jeunes gens un aperçu

de la grande aventure humaine qu'est l'aventure des nombres.

Transparent VII

REPOS

REPOS : J'avais décidé de ne pas préparer ce que je dirais du repos. J'ai quand même préparé quelques idées, comme cela, dans le train [Transparent VII].

Je vous ai fait faire **deux toutes petites promenades dans une grande jungle**, et vous avez vous-mêmes conscience que nous n'avons découvert que quelques tout petits îlots de cette jungle.

Vous vous attendiez, sans doute, à ce que je vous parle de **N**, de **Z**, de **Q**, de **R**, de **C**, des quaternions, des octavons. Non, il n'a été question de rien du tout, rien du tout de tout cela ! Aucune des structures qui apparaissent dans la théorie des nombres : je ne vous ai pas fait dépasser **N**, en allant vers les ordinaux infinis et les cardinaux infinis de Cantor. Je ne vous ai pas parlé d'arithmétique non standard. Je ne vous ai pas fait découvrir le champ énorme de cette espèce de pseudo-arithmétique qu'est la recherche des corps finis qui a été l'un des grands succès des mathématiques contemporaines.

Je ne vous ai pas parlé de nombres particuliers sur lesquels il y a tant à dire. Mais là, j'ai une excuse : vous invitez Jean-Paul Delahaye en janvier prochain. Il est l'auteur d'un livre sur *le fascinant nombre* π qui a reçu le Prix d'Alembert de la Société Mathématique de France. C'est un excellent livre : on peut voir comment sur un nombre tout seul, il est possible de regarder une foule de choses, en particulier la théorie de la transcendance, solution du vieux problème de la quadrature du cercle, et puis des propriétés asymptotiques qui font intervenir les notions de complexité en arithmétique et en informatique.

Et puis là où vraiment je dois vous paraître être au-dessous de tout, c'est que je n'ai même pas évoqué le « théorème de Fermat » et le théorème d'Andrew Wiles sur $a^n+b^n = c^n$. Bon, eh bien voilà, maintenant c'est fait, il est évoqué ! C'est vrai, c'est quand même l'un des grands triomphes des mathématiques contemporaines. Non pas par l'importance du résultat, car à partir du moment où il est démontré ce théorème n'a plus de valeur ; il est beaucoup moins important que le théorème $a^p = a$ modulo p dont je vous parlais tout à l'heure. Mais simplement parce que c'était le prototype d'une équation diophantienne qu'on ne savait pas comment résoudre. Une équation diophantienne, cela veut dire recherche des points rationnels sur les courbes algébriques. Recherche des points rationnels sur les courbes algébriques, cela veut dire géométrie algébrique. Les méthodes pour ces choses-là remontent à Euler pour une part, à Kummer avec l'introduction des nombres idéaux au XIX^e siècle, qu'on appelle maintenant tout simplement les idéaux ; et puis toutes les mathématiques développées par Andrew Wiles, l'arsenal... ce n'est pas la peine que je dise les « gros mots », mais les premières communications de Wiles ne s'appelaient pas démonstration du théorème de Fermat. Cela s'appelait *courbes elliptiques, formes modulaires et représentations galoisiennes*. Il « cachait » un petit peu.

Donc, j'ai choisi que nous fassions une promenade ensemble, parce que c'était la fin de la matinée, qu'il fallait vous préparer à une après-midi dure, de travail, et j'espère que la promenade n'était pas trop fatigante. Et le repos, eh bien, il doit être parfaitement reposant !

Je voudrais faire **une remarque** : quand j'avais proposé ce titre, *le nombre, cet inconnu*, je ne savais absolument pas de quoi j'allais parler. J'aurais pu choisir beaucoup d'autres sujets en théorie des nombres. Jean Souville a fait allusion au fait que ma spécialité est l'analyse de Fourier et l'analyse harmonique : il y a beaucoup de rapports entre théorie des nombres et analyse harmonique. J'aurais pu choisir de vous parler de cela. Mais sur n'importe quel sujet d'apparence élémentaire ; nombre, cercle, triangle, polyèdre..., vous demandez à un mathématicien de vous parler de ce qui l'intéresse, et vous obtenez un laïus semblable à celui que je viens de vous faire, sauf que, selon les mathématiciens, vous obtiendrez différents laïus. Si maintenant vous demandez à un mathématicien de Poitiers, spécialiste ou non en théorie des nombres, de vous parler du *nombre cet inconnu*, il vous fera un laïus complètement indépendant de celui que je vous est fait. Même chose en ce qui concerne le cercle, même chose en ce qui concerne le triangle.

Mais pour en revenir au nombre, la richesse des nombres pour nous tous, c'est que **les nombres sont très très liés à notre cerveau et à la civilisation humaine**. Pour notre cerveau, je n'en dirai pas plus, je renvoie simplement à un très très beau livre au très très mauvais titre, c'est Dehaene : *La bosse des maths*. C'est un livre absolument superbe, où vous voyez la notion de nombre s'introduire chez les animaux, s'introduire chez les enfants, les neurones spécialisés dans la reconnaissance des nombres, les localisations cérébrales correspondant à différentes mémoires des nombres. Je ne vais pas vous en parler.

Mais il faut quand même dire que les nombres sont extrêmement liés à toute la civilisation humaine, à la parole et à l'écriture. Pour la parole : vous avez certainement remarqué que « compter » et « conter », au sens de raconter, sont homonymes en français. En espagnol, ce n'est pas seulement qu'il sont homonymes, cela s'écrit de la même façon « contar ». En allemand « compter » c'est « zählen », « raconter » c'est « erzählen ».

Les nombres se racontent : « Il était une fois... 7 petits nains, 3 petits cochons, la bandes des 4, les 10 000 bouddhas...» Les nombres se racontent et **les comptines se chantent**. La table de multiplication, au Japon encore, se récite en chantant : c'est une chanson collective. Alors, je n'en dis pas plus. Et puis **les nombres s'écrivent**. Les plus anciennes traces d'écriture : les Sumériens avec l'écriture cunéiforme, les Babyloniens, ce sont les nombres. Chez les Chinois, également, avec l'apparition de l'écriture décimale, pas de l'écriture avec les zéros, mais l'apparition des chiffres de 1 à 9 et l'apparition de symboles pour désigner les dizaines, les centaines, les milliers les dizaines de milliers, sur les carapaces de tortues qu'on a conservées de la dynastie Shang datent du II^e millénaire avant J.-C.

Les nombres au cours de l'histoire..., la façon dont les Grecs les écrivaient, et l'apparition en force de la numération décimale avec Simon Stevin au cours du XVI^e siècle, avec immédiatement l'apparition des tables de logarithmes et des tables de nombres naturels : suivant immédiatement l'apparition de l'écriture décimale pour écrire de longs développements et faire des tables utilisées en navigation, avec les fonctions élémentaires telles qu'elles nous apparaissent encore aujourd'hui.

Alors, naturellement, ce que je vous dis là, c'est juste pour vous dire qu'**on a changé d'échelle**, que maintenant, on manipule des nombres beaucoup plus grands. Les physiciens vont des « pico » aux « téra », et pas seulement des « milli » aux « kilo ». Et puis, les enfants jonglent avec les puissances de 10 et avec des écritures très longues. L'informatique donne maintenant accès à une écriture de nombres très grands. Il est évident que cela change complètement la façon même dont les enfants appréhendent les nombres.

Les modes de calcul ont complètement changé. Il faut tout naturellement en tirer la conséquence, non pas seulement dans l'enseignement, mais pour toute notre civilisation à venir.

Voilà. Avant de terminer , je voudrais revenir à un mot que j'ai dit tout à l'heure à propos des nombres de Skewes, à savoir que, vraiment, ce **nombre gigantesque**, ce n'est pas très « naturel ». Il y a toutes sortes de pièges dans la dénomination des nombres. Il y a les « pièges négatifs », les nombres que l'on appelle « imaginaires », « irrationnels », « transcendants », « idéaux » ; et puis il y a les pièges pires que j'appellerai les « pièges positifs », les nombres qu'on appelle « réels », comme s'ils avaient une réalité plus que les nombres complexes, les nombres que l'on appelle « naturels », comme si réellement ils étaient naturels. Non ! Les nombres naturels sont **une merveilleuse création humaine**.

Le fait d'ajouter $+1$, cela, nous ne le connaissons pas dans le règne animal ; cela nous ne le connaissons pas chez les petits enfants. Mais le fait d'ajouter $+1$, c'est évidemment le premier accès à l'infini. Ce n'est pas seulement l'axiomatique de Peano, c'est le fait d'avoir accès à des nombres toujours plus grands. Et le fait que nous ayons accès à de très grands nombres maintenant avec les outils modernes, eh bien, c’est un grand acquis aussi de la civilisation !

Et ce que je voudrais donner comme impression de cette conférence, qui maintenant commence à être sacrément trop longue, c’est que j’aimerais bien, nous aimerions bien que, autour de nous et dans l’enseignement, cette « aventure des nombres » dont parle Godefroy, dans un très bon livre aussi, que j’ai eu le tort de ne pas signaler – G. Godefroy, *L’aventure des nombres* –, eh bien, que cette aventure des nombres si multiforme nous apparaisse comme un grand aspect de toute l’aventure humaine !