MATHÉMATIQUES

La quête des décimales de π

Boris Gourévitch[1]

Introduction

Le nombre π occupe une place très particulière dans le monde mathématique, et sans cesse réaffirmée. Il peut se targuer d'avoir occupé l'esprit des mathématiciens dès l'Antiquité, et comme le disent Bergrenn et les frères Borwein [6], le calcul de ses décimales est probablement le seul problème apparu dès les prémices des mathématiques, et qui soit encore d'actualité dans la recherche moderne. Pourtant, les motivations associées ont sensiblement évolué au cours des siècles.

D'abord liées aux besoins pratiques et quotidiens des anciens, les évaluations toujours plus précises du nombre π ont ensuite découlé, presque comme un jeu, des découvertes successives et foisonnantes de formules d'analyse toujours plus efficaces de la Renaissance jusqu'au XIXe siècle.

La révolution des ordinateurs au XXe siècle changea ensuite complètement la donne : l'attrait du calcul ne venait plus du résultat en lui-même, mais de la manière de l'obtenir, du point de vue des techniques mathématiques et algorithmiques. Un nouveau changement de cap a fait son apparition depuis 1996, qui tente de mettre en relation les expressions analytiques de π et la structure profonde de ses décimales. De ce champ d'explorations à la frontière de la théorie de la complexité ont éclos quelques conjectures encore ouvertes sur la nature « aléatoire » de nombreuses constantes mathématiques (π, $\ln(2)$, etc). D'autres conséquences jusqu'ici insoupçonnées, comme la possibilité d'atteindre dans certaines bases le n-ième chiffre de π sans connaître les précédents avec peu de mémoire et de temps, ont renouvelé l'attrait du calcul des chiffres ou décimales du nombre π.

Cet article se propose de revenir sur ces quatre périodes charnières (Antiquité, XVIIIe/XIXe siècle, XXe siècle, et depuis 1996) en expliquant les cheminements de pensée et les méthodes de calcul qui ont conduit à connaître plus de 1241.10^9 décimales de π en ce début de troisième millénaire ! Nous laisserons de côté les algorithmes et séries liées à π n'ayant pas servi au calcul de ses décimales, vu l'imagination foisonnante des mathématiciens dans ce domaine. Nous achèverons cette synthèse par un petit état des lieux des motivations actuelles de calcul des décimales de π.

[1] LTSI de l'université de Rennes I. Mél : `boris@pi314.net`

π dans l'Antiquité

Même si les symboles des mathématiques modernes ($=$, ^{2}, $\sqrt{}$, ...) n'ont fait leur apparition qu'à la Renaissance, il nous sera plus facile de les manipuler pour traduire les idées des anciens, qui décrivaient la plupart de leurs opérations avec des mots !

Des motivations pratiques

Les anciens avaient essentiellement besoin de la géométrie pour les mesures de surface de terre, ou dans l'architecture, par exemple pour évaluer la taille et la proportion des bâtiments. Selon l'historien grec Hérodote, on pouvait trouver de nombreuses relations géométriques dans les pyramides de Gizeh, à qui il rendit visite vers 450 av. J.C. (soit plus de 2000 ans après leur construction tout de même !). Par exemple, un principe de construction voulait que l'aire de chaque surface latérale soit égale à l'aire d'un carré de côté égal à la hauteur de la pyramide (ce qui est vrai à 0,7% près pour la pyramide de Kheops !). De nombreuses constantes apparaissent ainsi de manière quasi-magique, puisque le rapport de la hauteur sur le côté de la base de la pyramide vaut $\frac{\pi}{2}$ à 1,7% près. Ces coïncidences remarquables sont parfois contestées mais restent fascinantes.

Le plus ancien objet où π intervient plus ou moins implicitement est une tablette babylonienne en écriture cunéiforme, découverte en 1936 et qui remonte à la période 1900-1600 avant J.C. Elle évalue le périmètre d'un hexagone à $\frac{24}{25}$ fois celui du cercle circonscrit (soit $[0, 57, 36]$ dans leur base 60 dont il nous reste le décompte des secondes/minutes), ce qui revient à estimer $\pi_{Babylone} = 3\frac{1}{8} = 3.125$. C'est officiellement la plus vieille approximation connue de π !

De même, pour revenir aux Égyptiens, le célèbre papyrus de Rhind rédigé en écriture hiératique et découvert en 1855 par A. H. Rhind à Louxor relate une série de problèmes anciens recopiés par le scribe Ahmes. Le n° 50 affirme que l'aire d'un disque de diamètre 9 est égale à 64, soit le carré du diamètre auquel on a retiré $\frac{1}{9}$ de sa longueur$\left(9 - \frac{1}{9}.9\right)$. Ceci revient à estimer $\pi_{Égypte} = \left(\frac{16}{9}\right)^2 = 3.1604....$ Ils sont probablement parvenus à cette idée en approchant l'aire de ce disque par celle d'un octogone partitionné en carrés et triangles de côté 1, et qui donne alors une aire de 63 (problème n° 48). Notons que les Égyptiens ne travaillaient qu'avec des fractions de la forme $\frac{1}{n}$ et qu'ils avaient donc opté pour la meilleure des approximations de ce genre puisque la diminution du $\frac{1}{9}$ est meilleure que la diminition du $\frac{1}{8}$. Nous savons par ailleurs que les Égyptiens avaient compris que le rapport lié au périmètre d'un cercle et celui lié à l'aire du cercle étaient les mêmes.

Nous ne savons pas si c'était le cas des Babyloniens, ni même si ces civilisations avaient conscience de n'avoir obtenu qu'une valeur approchée de π. Les méthodes en Inde ancienne (600 avant J.C.) et Chine (150 après J.C.) semblent avoir été identiques. Il faut noter que la diffusion des connaissances étant plutôt réduite à cette époque, de nombreuses autres approximations, parfois bien plus mauvaises ($\pi = 3$ dans la Bible par exemple !) ont éclos même après la découverte de ces premières valeurs.

Le principe d'exhaustion chez les Grecs

Les mathématiciens grecs de l'Antiquité sont souvent considérés comme les premiers à réellement se soucier des démonstrations. Les problèmes qui les occupaient restaient cependant majoritairement géométriques. Parmi eux, le problème

de construire un carré de même aire qu'un cercle (la célèbre quadrature du cercle) fut initié, au moins historiquement, par Anaxagore (500-428 avant J.C.) pendant un séjour en prison pour impiété (il osait soutenir en particulier que la lune ne faisait que refléter la lumière du soleil !). Si de nombreuses solutions furent alors proposées, le problème devint insoluble pendant 23 siècles quand Euclide ajouta comme conditions de le résoudre uniquement :

(1) à l'aide d'une règle non graduée et d'un compas,
(2) en un nombre fini d'étapes (implicitement).

En fait, la règle n'est pas nécessaire dès que l'on dispose d'un compas (Mohr, 1762).

Le lien entre ces conditions et les propriétés algébriques des nombres qui en découlent ne fut proprement énoncé qu'en 1832 par Pierre Laurent Wantzel :

Théorème. — *L'ensemble des nombres constructibles au compas est le plus petit sous-corps de $\mathbb{C}$ stable par conjugaison et racine carrée.*

Bien que ces nombres soient algébriques (racines de polynômes à coefficients dans $\mathbb{Z}$), Abel montra en 1824 que tous les nombres algébriques ne sont pas toujours exprimables par radicaux – donc a *fortiori* constructibles au compas – dès que le degré du polynôme atteint 5, et Liouville démontra en 1851 l'existence de nombres non algébriques, *i.e.* transcendants. Le problème de la quadrature du cercle se ramena donc rapidement au milieu du XXe siècle à celui de la transcendance de π.

La distance qui séparait les conceptions géométriques grecques de l'expression formelle du problème de la quadrature du cercle explique la lente maturation des mathématiciens vers la démonstration finale et rigoureuse de la transcendance de π en 1882 par Lindemann, qui clôtura ce débat vieux de plus de 23 siècles !

Avec les outils dont disposaient les Grecs, les solutions proposées à la quadrature du cercle faisaient la plupart du temps appel à un nombre infini d'étapes comme la quadratrice de Dinostrate, construite initialement par Hippias d'Elis vers 430 avant J.C., ou encore la méthode d'exhaustion.

Cette dernière est généralement attribuée à Antiphon (vers 430 avant J.C.) ou Eudoxe de Cnide (408-355 avant J.C.), et consiste à construire un polygone dont le nombre de côtés augmenterait jusqu'à ce qu'il devienne indiscernable du cercle. Cette brillante idée se heurte néanmoins au manque de notion de limite à l'époque. Même si un polygone à n côtés est quarrable, cela ne signifie pas que sa limite – le cercle – le soit aussi, contrairement à l'idée d'Antiphon. Le brillant Euclide (330-275 avant J.C.) écrit néanmoins qu'en considérant un polygone avec un grand nombre de côtés, on peut « rendre la différence entre l'aire à calculer et l'aire des polygones qu'on construit plus petite que toute quantité positive pré-assignée, aussi petite soit-elle » (d'après [12]), ce qui est une conception étonnament proche de la formalisation des limites dans les mathématiques du XXe siècle. Il en déduisit d'ailleurs que l'aire du cercle était proportionnelle au carré de son diamètre (Éléments 12.2).

Il faut cependant attendre Archimède (287-212 avant J.C.) et son traité *De la mesure du cercle* pour que cette idée soit efficacement appliquée à l'évaluation de π. Le premier de ses trois théorèmes énonce que le rapport de l'aire d'un disque

au carré de son rayon est égal au rapport du périmètre à son diamètre. Le troisième énonce explicitement que

$$3 + \frac{1}{7} < \pi < 3 + \frac{10}{71}. \tag{1}$$

Reprenant le principe d'exhaustion, il exhibe une relation formelle entre le périmètre du polygone à n côtés et celui à $2n$ côtés. Partant de deux hexagones respectivement inscrit et circonscrit, il obtient l'approximation (1) avec deux polygones à 96 côtés ! Ce calcul absolument sidérant fut mené sans aucune notation algébrique, numération cohérente (les Grecs utilisaient une numération additive comme les Romains), ni connaissance de la trigonométrie, et avec la seule géométrie d'Euclide. Il se formalise aujourd'hui comme suit : soient a_n et b_n les demi-périmètres des polygones à 3.2^n côtés respectivement circonscrit et inscrit à un cercle de rayon 1. L'hexagone fournit $a_1 = 2\sqrt{3}$ et $b_1 = 3$. On a ensuite les formules de récurrence

$$a_{n+1} = \frac{2a_n b_n}{a_n + b_n} \qquad , \qquad b_{n+1} = \sqrt{a_{n+1} b_n}$$

qui donnent $\pi = \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$. Archimède poussa ses calculs jusqu'à $n = 5$. Les cas $n = 1$ et $n = 2$ sont illustrés sur la figure 1. La démonstration de la

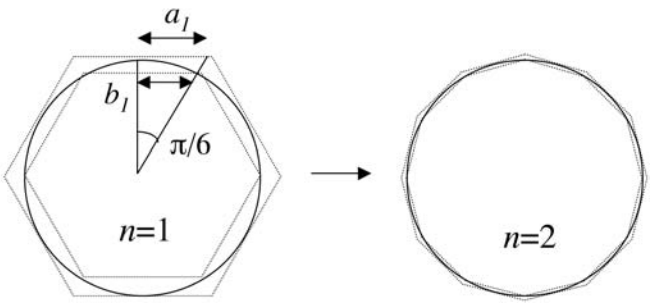

Fig. 1 Approximation du cercle par des polygones inscrit et circonscrit. Cas $n = 1$ et $n = 2$ de l'itération d'Archimède.

convergence et de l'adjacence des deux suites est immédiate si l'on remarque que $a_n = 3.2^n \tan\left(\frac{\pi}{3.2^n}\right)$ et $b_n = 3.2^n \sin\left(\frac{\pi}{3.2^n}\right)$. On obtient alors

$$a_n - b_n = 3.2^n \tan\left(\frac{\pi}{3.2^n}\right)\left(1 - \cos\left(\frac{\pi}{3.2^n}\right)\right) = \frac{\pi^3}{18.4^n} + o\left(\frac{1}{4^n}\right)$$

ce qui assure $\frac{3n}{5}$ décimales correctes en n itérations environ (3 décimales en 5 étapes). On qualifiera cette convergence de linéaire. Le rayonnement d'Archimède était déjà tel pour l'époque, que Tropfke [25] affirme que la valeur $\pi_{Grecs} = 3\frac{1}{7}$ remplaça rapidement à Alexandrie la vieille valeur $\pi = \left(\frac{16}{9}\right)^2$, d'usage aussi aisé mais moins précise, et se répandit jusqu'en Inde et même en Chine au Ve siècle après J.C.

Deux millénaires d'attente

Après Archimède, les mathématiciens occidentaux mais aussi asiatiques, arabes ou indiens, se contenteront d'appliquer la même méthode ou une variante légère pendant près de 20 siècles. Descartes (1596-1650) propose sa méthode des isopérimètres qui fait non plus évoluer le périmètre des polygones mais bien le diamètre de ces polygones, dont le périmètre est alors fixé. Viète dérive tout de même un premier produit infini en 1593 en se penchant sur l'aire et non plus le périmètre.

Poussant le calcul plus loin qu'Archimède, le record en la matière appartient à Ludolph Van Ceulen, qui exhiba 20 décimales en 1596 à l'aide de polygones à $60.2^{33} = 480$ milliards de côtés, puis 32 décimales à l'aide de polygones à 2^{62} côtés dans une publication posthume de 1615, pour enfin se voir attribuer et graver sur sa pierre tombale 35 décimales en 1621. Autant dire qu'il passa sa vie à cet exercice !

En fait il n'y eut guère de progrès réel pendant cette période essentiellement à cause de l'utilisation exclusive de l'approche géométrique, qui trouvait là ses limites dans le calcul des décimales de π.

L'apport des séries à la Renaissance

Le grand tournant eut lieu avec la manipulation de plus en plus courante de sommes et de produits infinis dans le monde mathématique de la fin du Moyen-Âge. Bien avant les européens, on attribue aux indiens les premières expressions de π sous forme de série puisque l'on trouve déjà dans les écrits en sanscrit des disciples de Nilakantha Somayaji (1444-1545 !) la formule

$$\pi = \sqrt{12}\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)3^n} \tag{2}$$

parmi huit autres. Sa simplicité et sa rapidité de convergence (environ $\frac{n}{2}$ décimales correctes pour n termes) aurait déjà pu mener les mathématiciens de cette époque à connaître des dizaines de décimales de π ! Pourtant, à cette époque, c'est Al-Kashi de Samarkande qui vient de réussir le tour de force de calculer 14 décimales de π en 1429 à l'aide d'une variante de la méthode d'Archimède et en système sexagésimal. Plus fort encore, alors que James Gregory (1638-1675) fait enfin profiter l'Europe de la découverte du développement en série entière de la fonction arctan

$$\arctan(x) = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)} \tag{3}$$

en 1671, c'est Abraham Sharp (1651-1742) qui utilise le cas particulier $\frac{\pi}{6} = \arctan\left(\frac{1}{\sqrt{3}}\right)$, autrement dit l'équation (2), pour obtenir 71 décimales correctes de π en 1699, près de 200 ans après Nilakantha ! Le développement d'arcsin fut obtenu par Newton vers 1665-1666, qui en profita pour calculer 15 décimales de π, n'ayant « *rien d'autre à faire* » comme il l'affirma lui-même.

La fonction arctan est un bon candidat pour le calcul des décimales de π à la main car si l'on s'y prend bien, on n'utilise que des termes rationnels ou au plus

une racine comme dans (2). Ainsi John Machin (1680-1752) parvient aisément à 100 décimales en 1706 en proposant la désormais célèbre formule

$$\frac{\pi}{4} = 4.\arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{239}\right). \tag{4}$$

La démonstration ou la recherche de ce type de formules (dont quatre autres exemples sont donnés plus loin par les équations (6), (7), (23) et (24) s'obtient grâce à la règle suivante

Théorème. — *Soient $a_1, a_2, ..., a_p$ et $b_1, b_2, ..., b_p$ des entiers, les a_j étant non nuls.*
$\sum_{j=1}^{p} \arctan\left(\frac{b_j}{a_j}\right) = k\pi$, *$k \in \mathbb{Z}$, si et seulement si* $\Im m\left(\prod_{j=1}^{p}(a_j + i \cdot b_j)\right) = 0$.

Démonstration. Si $c_j = a_j + i.b_j \in \mathbb{C}^*$, $\sum_{j=1}^{p} \arctan\left(\frac{b_j}{a_j}\right)$ est un argument de $\prod_{j=1}^{p} c_j$. □

La rapidité de convergence de ces formules est contrainte par le plus grand terme $\frac{b_j}{a_j}$ et d'après l'équation (3), on obtient une convergence linéaire en utilisant n termes du développement de Taylor de la fonction arctan. Désormais, les combinaisons d'arctan vont servir de base à la course aux décimales jusqu'en 1985 ! Il faut cependant remarquer qu'à partir de Newton, ce sont – sans leur faire injure – plutôt des mathématiciens de second plan qui se battront pour le record. D'ailleurs, le nombre de décimales déjà calculé en ces temps est bien supérieur aux véritables besoins des mathématiciens et des physiciens. On estime en effet que pour calculer la circonférence de l'univers avec la précision d'un atome d'hydrogène, seules 39 décimales de π sont requises ! [1] Les motivations sont donc plutôt tournées vers la recherche de périodicités ou motifs dans les décimales de π. Sachant que la périodicité des décimales d'un nombre en fait un rationnel (fraction de deux entiers), cette première question est tranchée en 1761 avec la démonstration de l'irrationnalité de π par Johann Lambert (1728-1777). Sa démonstration plutôt lourde s'appuie sur un développement en fraction continue de la fonction tan. Les limites « humaines » de calcul des décimales à la main semblent atteintes en 1874 avec l'obtention de 707 décimales par Shanks, qui sont d'ailleurs fausses à partir de la 528e. Ferguson le remarquera près de 70 ans plus tard en les comparant aux 808 qu'il obtint en 1948, avec les premières machines à calculer (des additionneurs en fait, hérités du principe de celle mécanique construite par Leibniz dès 1694).

L'ordinateur prend le relais

Le souffle indien

Durant la première moitié du XXe siècle, les préoccupations mathématiques sont ailleurs. Les théories élaborées par Cantor, Gödel, Kolmogorov, la topologie et la liste des 23 problèmes de Hilbert ouvrent tout-à-coup des horizons qui donnent un coup de vieux à l'analyse classique. Celle-ci semblait pourtant avoir trouvé son évolution naturelle dans l'étude des intégrales elliptiques menées par Legendre, puis Gauss, Abel et Jacobi durant la première moitié du XIXe siècle.

Fig. 2 Srinivasa Ramanujan (1887-1920)

Heureusement un génie né au fin fond de l'Inde en 1887, Srinivasa Ramanujan (fig. 2), va se charger de donner un souffle nouveau aux recherches menées autour de π. Lui-même passionné par cette constante, c'est un autodidacte complet qui passa les 25 premières années de sa vie à reconstruire les mathématiques à partir d'un unique ouvrage de 6165 théorèmes sans démonstration ("Synopsis of elementary results in pure and applied mathematics" de G.S.Carr). Cet état d'esprit le conduisit à énoncer la plupart de ses résultats sans démonstration (ce qui ne signifie pas qu'il ne comprenait pas d'où ils venaient !). Doté d'une intuition exceptionnelle qui lui permit de progresser à pas de géants dans la théorie des nombres et des équations modulaires, il découvrit des formules venues d'ailleurs comme celle-ci publiée en 1914

$$\pi = \frac{9801}{\sqrt{8}} \left(\sum_{n=0}^{\infty} \frac{(4n)!(1103 + 26390n)}{(n!)^4 (396)^{4n}} \right)^{-1}. \tag{5}$$

Il existe une anecdote célèbre à propos de cette formule : sa démonstration presque entière fut achevée au début des années quatre-vingt par les frères Borwein [7]. Il restait le coefficient 1 103 à justifier, il devait être entier, mais la longueur des calculs et équations requises était épouvantable. Gosper effectua alors en 1985 un calcul « à l'aveugle » de 17 millions de décimales de π à l'aide de cette formule. Aussi vrai que deux entiers proches de moins d'une unité sont égaux, la concordance des résultats du calcul de Gosper avec les 10 millions de décimales déjà connues à l'époque constitua une démonstration finale de la formule de Ramanujan ! On suppose que Ramanujan avait dû procéder de même sur quelques décimales.

Les Borwein tireront des travaux de Ramanujan une ribambelle d'algorithmes remarquables assez largement utilisés de nos jours dans le calcul des décimales de π (voir paragraphe page 45). La complexité de la démonstration d'une telle formule est telle que malheureusement même un survol des résultats, sans démonstration des intermédiaires, occupe au minimum une dizaine de pages dans le remarquable ouvrage [13]. Le lecteur intéressé par une plongée dans l'univers passionnant des équations modulaires, corps quadratiques, et autres intégrales elliptiques pourra se référer à la « Bible » [7], d'une pédagogie remarquable.

Ramanujan fut repéré par le mathématicien anglais Hardy auquel il avait écrit une lettre en 1913, s'embarqua pour l'Angleterre en 1914 et leur collaboration

fructueuse dura jusqu'en 1919. Il repartit alors en Inde où il mourut l'année suivante, probablement de carences en vitamines. Considéré comme un des plus grands génies du XXe siècle, Ramanujan a laissé des carnets remplis de formules en notations non-standards, dont le déchiffrage s'est poursuivi jusqu'à nos jours (!), d'abord assuré par Bruce Berndt, puis par les frères Borwein.

La course aux décimales reprend

Après la guerre, l'avènement des machines à calculer fait progresser la course aux décimales à pas de géants ! Ferguson ouvre le bal en 1946 en obtenant 620 décimales à l'aide d'un calculateur de bureau. Le premier calcul sur ordinateur est confié au fameux ENIAC en 1949 qui rend 2037 décimales en 70 heures à l'aide de la formule de Machin (4). En 1973, Guilloud et Bouyer atteignent le premier million de décimales sur CDC 7600 à l'aide de deux formules d'arctan célèbres, celles de Gauss (6) et de Störmer (7).

$$\frac{\pi}{4} = 12.\arctan\left(\frac{1}{18}\right) + 8.\arctan\left(\frac{1}{57}\right) - 5.\arctan\left(\frac{1}{239}\right) \tag{6}$$

$$\frac{\pi}{4} = 6.\arctan\left(\frac{1}{8}\right) + 2.\arctan\left(\frac{1}{57}\right) + \arctan\left(\frac{1}{239}\right) \tag{7}$$

Le calcul en binaire prit respectivement 22h11 et 13h40, et la conversion en base décimale 1h07. Un livre de 415 pages de décimales tiré de ce calcul fut qualifié à l'époque de « livre le plus ennuyeux du monde » !

Il faut noter que le processus attaché à la course aux décimales est toujours le même jusqu'à aujourd'hui : les calculs sont effectués avec deux formules distinctes puis comparés pour validation du record. Les figures 3 et 4 montrent l'évolution des records de calcul de décimales de π au cours des siècles.

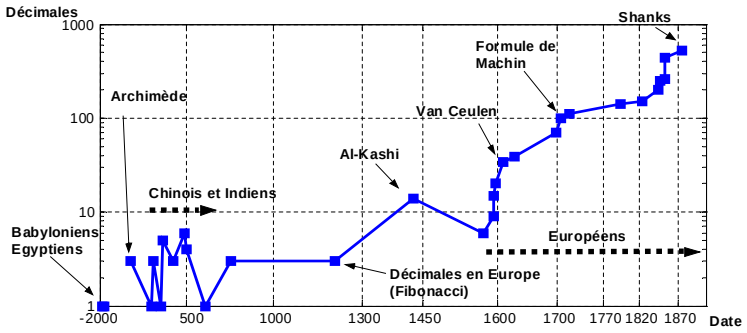

Fig. 3 Nombre de décimales calculées à la main dans l'histoire.
Les échelles sont logarithmiques.

Améliorations algorithmiques

Dans les années cinquante à soixante-dix, le manque d'algorithme de multiplication efficace oblige à segmenter chaque nombre en tranches, par exemple $B = B_2 10^{20} + B_1 10^{10} + B_0$. La multiplication de nombres de taille n nécessite alors un temps (ou nombre d'opérations) proportionnel à n^2 sans compter l'utilisation mémoire proportionnelle à n. Sans des améliorations théoriques et algorithmiques,

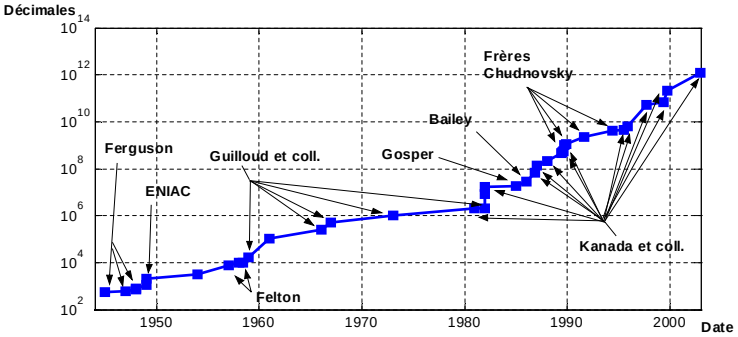

Fig. 4 Nombre de décimales obtenues à l'aide de calculateurs ou d'ordinateurs au XXe siècle. L'échelle des décimales est logarithmique.

la progression du record de décimales aurait donc été très lente. C'est alors à cette époque que les choses s'accélèrent.

En 1965, Cooley et Tukey introduisent sous sa forme moderne une méthode de réduction de la complexité du calcul des séries de Fourier connue aujourd'hui sous le nom de Transformée de Fourier Rapide [11]. Schönhage et Strassen en tirent en 1971 un algorithme de multiplication de grands entiers en complexité $O\left(n.log(n).log(log(n))\right)$ ce qui est considérablement mieux que $O\left(n^2\right)$ [24] !

En 1976, Salamin et Brent parviennent indépendamment au même algorithme ([23, 8])

$$\begin{aligned} a_0 &= 1, \quad b_0 = \frac{1}{\sqrt{2}} \\ a_{n+1} &= \frac{a_n + b_n}{2}, \quad b_{n+1} = \sqrt{a_n b_n} \\ U_n &= \frac{2a_n^2}{1 - \sum_{k=0}^{n} 2^k \left(a_k^2 - b_k^2\right)}, \quad \pi = \lim_{n\to\infty} U_n \end{aligned} \tag{8}$$

qui a une propriété extraordinaire de convergence quadratique, autrement dit le nombre de décimales exactes double à chaque itération.

Ajoutons enfin que l'algorithme de Newton, proposé vers 1669 (!), ramène la division et l'extraction de racines carrées à des multiplications et propose une convergence elle aussi quadratique. Autant dire que tous les ingrédients sont réunis pour faire exploser les records !

La compétition reprend en effet en 1981 avec Myioshi et Kanada (2 000 036 décimales) et dès la fin de 1982, on en connaît 16 777 206 (Kanada, Yochino et Tamura). La lutte concernera ensuite principalement Kanada et, entre 1991 et 1994, les deux frères David et Gregory Chudnovsky qui utiliseront une série de leur cru de type Ramanujan et un ordinateur dont ils ont eux-mêmes conçu l'architecture. Selon la légende, leur appartement new-yorkais contient des montagnes de papiers en désordre et est chauffé aux microprocesseurs ! Ces mathématiciens isolés mais au talent reconnu (Gregory est considéré comme un génie exceptionnel mais il est atteint d'une maladie l'empêchant de travailler en université) montrent au moins que des scientifiques de tout premier plan s'intéressent au calcul des décimales de π [12].

Arrêtons-nous maintenant sur les justifications des trois algorithmes de FFT, de Newton et de Brent-Salamin qui sont à la base des records de calcul successifs depuis le début des années quatre-vingt.

L'algorithme de multiplication rapide de deux grands entiers par FFT

Soient X et Y deux grands entiers de taille n en base $B = 10$ usuellement (ou une puissance de 10).

Décomposition polynomiale

On écrit X et Y sous forme polynomiale en les décomposant (de manière unique) dans la base B

$$X = P(B), \quad P(z) = \sum_{j=0}^{n-1} x_j z^j \tag{9}$$
$$Y = Q(B), \quad Q(z) = \sum_{j=0}^{n-1} y_j z^j$$

où x_j et y_j sont donc respectivement les j-ième chiffres en base B de X et Y ($0 \leqslant x_j, y_j \leqslant B-1$). Cette opération est de complexité à peu près proportionnelle à n. On cherche maintenant à effectuer « rapidement » la multiplication $R(z) = P(z) \times Q(z)$ puis à évaluer à la fin $R(B)$. $R(z)$ est un polynôme de degré $< 2n$ et peut être retrouvé par interpolation à partir de son évaluation en $2n$ points, autrement dit par l'évaluation de P et Q en ces mêmes $2n$ points. Le choix des points, c'est la finesse de l'algorithme ! On utilise les racines primitives $2n$-ièmes de l'unité, *i.e.* les

$$e^{\frac{2ik\pi}{2n}} = \omega^k, \qquad \omega = e^{\frac{i\pi}{n}}$$

car cette évaluation (qui n'est alors rien d'autre que le calcul d'une série de Fourier) peut être réalisée en complexité $O(n.\log n)$ si n est une puissance de 2 et avec un peu d'astuce. C'est la Transformée de Fourier Rapide ou FFT en anglais.

Transformée de Fourier rapide

En conservant les notations précédentes, évaluons le polynôme $P\left(\omega^k\right)$ et $Q\left(\omega^k\right)$ en se plaçant sous l'hypothèse que $n = 2^d$. Posons

$$P_1\left(z^2\right) = x_0 + x_2 z^2 + x_4 z^4 + \ldots + x_{n-2} z^{n-2}$$
$$P_2\left(z^2\right) = x_1 + x_3 z^2 + x_5 z^4 + \ldots + x_{n-1} z^{n-2}$$

et $y = z^2$. On obtient alors

$$P(z) = P_1(y) + z.P_2(y)\,. \tag{10}$$

Maintenant, il faut se rappeler que puisque ω est une racine $2n$-ième de l'unité, alors pour $k \in \{1, \ldots, 2n\}$,

$$\left(\omega^k\right)^2 = \left(\omega^{n+k}\right)^2.$$

En conséquence, évaluer P aux racines $2n$-ièmes de l'unité revient à évaluer P_1 et P_2 chacun aux n points $\left(\omega^2\right)^1, \left(\omega^2\right)^2, \ldots, \left(\omega^2\right)^n$ et à reporter les résultats dans P à l'aide de l'équation (10). Si $F(2n)$ est le nombre d'opérations élémentaires

(addition, multiplication) requises pour évaluer P en $\omega^1, \omega^2, \ldots, \omega^{2n}$ alors en vertu du principe précédent et de (10), on a

$$F(2n) = 2F(n) + 2 \times 2n, \quad F(1) = 0$$

où le terme $2 \times 2n$ provient des dernières addition et multiplication requises pour obtenir P à partir de P_1 et P_2 dans (10).

Comme ω^2 est une racine primitive n-ième de l'unité, on peut réappliquer le même procédé pour chaque polynôme P_1 et P_2. Par suite, comme $n = 2^d$ est une puissance de 2, le processus (et donc (10) s'itère encore d fois. On obtient finalement un nombre d'opérations

$$F(2n) = 2 \times 2n \times (d+1) = 4n \left(\frac{\log n}{\log 2} + 1 \right)$$

d'où la complexité en $O(n. \log n)$ de la FFT. De même pour la FFT inverse, qui utilise ω^{-k} au lieu de ω^k.

Interpolation

Nous avons maintenant calculé nos $P\left(\omega^k\right)$ et $Q\left(\omega^k\right)$ pour $k = 0, \ldots, 2n-1$. On forme les $2n$ produits $R\left(\omega^k\right) = P\left(\omega^k\right) Q\left(\omega^k\right)$ qui reviennent à des multiplications élémentaires puisque $P\left(\omega^k\right)$ est forcément de module inférieur à $\sum_{j=0}^{n-1} x_j \leqslant n(B-1)$ d'après (9), de même pour Q. Comme l'on cherche à retrouver $R(z) = \sum_{j=0}^{2n-1} r_j z^j$, il faut l'interpoler à partir des $2n$ valeurs $\alpha_k = R\left(\omega^k\right)$. Autrement dit, on cherche à résoudre le système

$$W\left(r_0, r_1, \ldots, r_{2n-1}\right) = \left(\alpha_0, \alpha_1, \ldots, \alpha_{2n-1}\right)$$

où

$$W = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & & \omega^{2n-1} \\ 1 & \omega^2 & \omega^4 & & \omega^{4n-2} \\ \vdots & & & & \vdots \\ 1 & \omega^{2n-1} & \omega^{4n-2} & & \omega^{2n^2-n} \end{pmatrix}$$

ce qui est équivalent à

$$\left(r_0, r_1, \ldots, r_{2n-1}\right) = W^{-1}\left(\alpha_0, \alpha_1, \ldots, \alpha_{2n-1}\right)$$

où W^{-1} a la bonne idée d'être simple

$$W^{-1} = \frac{1}{2n} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & & \omega^{-2n+1} \\ 1 & \omega^{-2} & \omega^{-4} & & \omega^{-4n+2} \\ \vdots & & & & \vdots \\ 1 & \omega^{-2n+1} & \omega^{-4n+2} & & \omega^{-2n^2+n} \end{pmatrix}.$$

Le calcul de $\left(r_0, r_1, \ldots, r_{2n-1}\right)$ n'est donc rien d'autre que le conjugué de la transformée de Fourier de $\left(\alpha_0, \alpha_1, \ldots, \alpha_{2n-1}\right)$, autrement dit sa transformée de Fourier inverse, dont on a vu qu'elle est en $O(n. \log n)$ comme la FFT. On obtient alors

$R(z)$ d'où l'on tire $R(B) = XY$. Cette dernière opération est à peu près en complexité $O(n)$ car les $r_0, r_1, \ldots, r_{2n-1}$ sont déjà proches des décimales de XY, aux retenues près (dès que $r_j \geqslant B$). Toutes les retenues sont en fait calculées simultanément, puis reportées, puis on recalcule les éventuelles nouvelles retenues créées, etc. (opération appelée vectorisation).

La combinaison de tous ces algorithmes et quelques menus raffinements selon les programmeurs permettent d'atteindre à peu près la borne optimale théorique de Schönhage et Strassen pour la FFT en $O\left(n.log(n).log(log(n))\right)$.

L'algorithme de Newton

Énoncé

L'algorithme de Newton, vieux de plus de trois siècles, est à l'origine utilisé pour approcher numériquement une racine a de l'équation $f(x) = 0$. Il permet en fait de montrer l'équivalence de la multiplication, la division et l'extraction de racines carrées d'un point de vue complexité.

Newton avait proposé dès 1669 un processus itératif pour trouver les racines d'équations polynomiales et Raphson le mit sous forme plus algorithmique en 1690. Simpson, Mourraille, Cauchy et Kantorovich ajoutèrent des raffinements et proposèrent des généralisations pour arriver à l'énoncé moderne suivant

Théorème. — *Soit f analytique dans un voisinage complexe de z. Supposons que $f(z) = 0$ et $f'(z) \neq 0$. Alors l'itération*

$$x_{k+1} = x_k - \frac{f\left(x_k\right)}{f'\left(x_k\right)}$$

converge uniformément et quadratiquement vers z pour une valeur initiale x_0 prise dans un voisinage de z.

Cet algorithme s'accompagne d'une propriété étonnante d'auto-compensation des erreurs : si x_k est perturbé et ne compte plus que M décimales justes par rapport à z alors le terme x_{k+1} contiendra tout de même $2M$ décimales exactes s'il a été calculé avec suffisamment de décimales, autrement dit la convergence quadratique sera préservée.

Une conséquence directe est que pour calculer z avec n décimales, il suffit d'initier l'algorithme avec quelques décimales au début et doubler la précision prise en compte à chaque itération jusqu'à atteindre une précision supérieure à n. Ceci simplifie considérablement la complexité de l'opération et permet de montrer que la multiplication, la division et l'extraction de racines carrées sont équivalentes en complexité.

Inverse d'un nombre

Prenons l'exemple d'un nombre $|y| \leqslant 1$ dont on souhaite calculer l'inverse avec $n = 2^d$ décimales exactes. En utilisant la fonction $f(x) = 1/x - y$, l'itération associée est

$$x_{k+1} = 2x_k - x_k^2 y \tag{11}$$

qui utilise uniquement des multiplications et additions. L'expression

$$x_{k+1} - \frac{1}{y} = -y\left(x_k - \frac{1}{y}\right)^2$$

illustre la convergence quadratique de l'algorithme. Initions maintenant l'itération avec une décimale exacte, soit

$$\left| x_0 - \frac{1}{y} \right| < \frac{1}{10}.$$

Grâce à la propriété d'auto-correction de la méthode de Newton, à l'itération k, on n'utilise que 2^k décimales pour les calculs. Et d'après (11), pour obtenir x_k, on a uniquement besoin de 2 multiplications ($x_{k-1} \times x_{k-1}$ et $x_{k-1}^2 y$) et 2 additions ($x_{k-1} + x_{k-1}$ et $2x_{k-1} - x_{k-1}^2 y$). En raison de la convergence quadratique, il suffira d'environ $log_2(n) = d$ itérations de (11) pour parvenir à n décimales exactes de $\frac{1}{y}$. Si on note $M(n)$ la complexité d'une méthode de multiplication pour n décimales, sachant que la complexité d'une addition sera n, on obtient alors une complexité finale de

$$\sum_{k=1}^{\log_2(n)} \left(2M\left(2^k\right) + 2.2^k\right) \leqslant 4M(n) + 4n \leqslant 8M(n). \tag{12}$$

Il est en effet raisonnable d'envisager $2M(p) \leqslant M(2p)$ autrement dit que la complexité de 2 multiplications de nombres à p décimales requiert un peu moins de complexité que la multiplication de deux nombres à $2p$ décimales. Ceci induit $2M\left(2^k\right) \leqslant M\left(2^{k+1}\right) \leqslant ... \leqslant \frac{1}{2^{d-k-1}} M(n)$ dans (12). L'inversion n'est donc guère plus compliquée que la multiplication (c'est un $O\left(M(n)\right)$) et comme $a.b = a.\frac{1}{b}$, la division est elle aussi un $O\left(M(n)\right)$.

Extraction de racines carrées

Les choses se passent aussi bien. On peut utiliser la fonction $f(x) = \frac{1}{x^2} - y$ qui conduit à l'approximation de $\frac{1}{\sqrt{y}}$ puis on fait $\sqrt{y} = y.\frac{1}{\sqrt{y}}$. L'itération associée est

$$x_{k+1} = x_k + x_k \frac{1 - y.x_k^2}{2}$$

ce qui conduit en pratique à une complexité finale d'environ $4M(n)$.

Une alternative plus naturelle est d'utiliser directement la fonction $f(x) = y - x^2$, mais cela conduit à une itération comprenant une division disqualifiante

$$x_{k+1} = x_k + \frac{y - x_k^2}{2x_k}.$$

Cependant, Schönhage, qui ne manquait pas d'idées, a proposé en 1971 de remplacer $\frac{1}{2x_k}$ par une approximation tirée d'une itération couplée et a obtenu

$$\begin{aligned} x_0 \approx \sqrt{y}, \qquad v_0 &= \frac{1}{2x_0} \\ v_{k+1} &= v_k + \left(1 - 2x_k v_k\right) v_k \\ x_{k+1} &= x_k + \left(y - x_k^2\right) v_{k+1}. \end{aligned}$$

Ce processus, où v_{k+1} estime $\frac{1}{2\sqrt{y}}$, est appelé « itération couplée de Newton » ([24], p. 257) et requiert en pratique une complexité d'environ $3M(n)$.

On trouvera de nombreux raffinements de la méthode de Newton dans [16, 1] et l'équivalence de la complexité de la multiplication, la division et l'extraction de racines est abordée dans [10, 8].

L'algorithme de Brent-Salamin

La moyenne arithmético-géométrique (AGM en anglais)

L'algorithme de Brent Salamin a une histoire extraordinaire. Il repose sur l'itération

$$a_0 = a \qquad b_0 = b$$
$$a_{k+1} = \frac{a_k + b_k}{2}, \qquad b_{k+1} = \sqrt{a_k b_k}. \tag{13}$$

avec $a_0, b_0 \in \mathbb{R}^{+*}$.

Les suites a_k et b_k sont adjacentes et convergent quadratiquement vers une valeur $M(a,b)$ appelée moyenne arithmético-géométrique et qui est encadrée par la moyenne arithmétique $\frac{a+b}{2}$ et la moyenne géométrique $\sqrt{ab}$.

Lagrange (1736-1813) fut le premier à utiliser l'itération pour l'approximation de certaines intégrales elliptiques, mais il n'en saisit visiblement pas la portée. Gauss découvrit l'AGM vers 1791 (à 14 ans !) et, fasciné, passa les dix années suivantes à défricher la théorie qui s'était ouverte devant lui. En 1797, il commença à travailler sur la courbe de la Lemniscate (d'équation polaire $r^2 = \cos 2\theta$) et remarqua numériquement le 30 mai 1799 que son demi-périmètre (noté usuellement ϖ et prononcé « pi script ») vérifiait sur 11 décimales la relation

$$\frac{\pi}{\varpi} = M(\sqrt{2}, 1).$$

Cette connexion improbable le rendit enthousiaste et lui permit de faire explicitement le lien avec les intégrales elliptiques. Il trouva enfin une expression générale de l'AGM sous forme intégrale à la fin de 1799 (deux preuves) et publia en 1818 une troisième preuve élégante, ici relatée, de la relation suivante :

Théorème. — *Notons* $I(a,b) = \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{a^2\cos^2\theta + b^2\sin^2\theta}}$ *l'intégrale elliptique complète de première espèce. On a*

$$M(a,b) = \frac{\pi}{2I(a,b)} \tag{14}$$

et $\varpi = 2I(\sqrt{2}, 1)$.

Démonstration. La substitution $t = b\tan\theta$ dans I induit que

$$I(a,b) = \frac{1}{2}\int_{-\infty}^{\infty} \frac{dt}{\sqrt{(a^2+t^2)(b^2+t^2)}}$$

puis le changement de variable $u = \frac{1}{2}(t - \frac{ab}{t})$ (et un peu de travail) conduisent à

$$I(a,b) = \frac{1}{2}\int_{-\infty}^{\infty} \frac{du}{\sqrt{(ab+u^2)\left(\left(\frac{a+b}{2}\right)^2 + u^2\right)}}$$

donc $I(a,b) = I\left(\sqrt{ab}, \frac{a+b}{2}\right)$ et il s'ensuit que d'après l'expression de l'AGM, $I(a,b) = I(a_1,b_1) = ... = I(a_n,b_n)$. Comme $\left(a_n^2\cos^2\theta + b_n^2\sin^2\theta\right)^{-\frac{1}{2}}$ converge uniformément vers $M(a,b)^{-1}$ si $n \to \infty$, on peut intervertir limite et intégrale dans $I(a,b)$ et obtenir

$$I(a,b) = \int_0^{\frac{\pi}{2}} \frac{d\theta}{M(a,b)} = \frac{\pi}{2M(a,b)}. \tag{15}$$

□

Bien que (14) fournisse une manière rapide d'évaluer $I(a,b)$ (moyennant la connaissance de π), on cherche surtout à éliminer $I(a,b)$ pour en tirer un algorithme convergeant vers π.

La relation de Legendre

On se sert pour cela de la fameuse relation de Legendre (1752-1833) :

Théorème. — *Introduisons l'intégrale elliptique complète de seconde espèce*

$$J(a,b) = \int_0^{\frac{\pi}{2}} \sqrt{a^2\cos^2\theta + b^2\sin^2\theta}\,d\theta = \int_0^{\frac{\pi}{2}} \frac{a^2\cos^2\theta + b^2\sin^2\theta}{\sqrt{a^2\cos^2\theta + b^2\sin^2\theta}}d\theta \tag{16}$$

qui représente la longueur du quart d'une ellipse d'axe majeur a et d'axe mineur b. Si le couple (b,b') est lié par la relation $b^2 + b'^2 = 1$, alors on a

$$L(b) = I(1,b)J(1,b') + I(1,b')J(1,b) - I(1,b)I(1,b') = \frac{\pi}{2}$$

Démonstration. Legendre a montré que la dérivée de $L(b)$ par rapport à b était nulle. La valeur constante de la fonction est ensuite obtenue en faisant tendre b vers 0. □

L'algorithme pour π

L'idée est maintenant de trouver un lien entre $I(a,b)$ et $J(a,b)$ pour éliminer J dans la relation de Legendre. Fort opportunément, on a

Théorème. —

$$J(a,b) = \left(a^2 - \frac{1}{2}\sum_{k=0}^{\infty} 2^k\left(a_k^2 - b_k^2\right)\right) I(a,b) \tag{17}$$

en reprenant les notations de (13).

Démonstration. De la même manière que pour I, on montre que

$$J(a,b) = 2J\left(\frac{a+b}{2}, \sqrt{ab}\right) - a.b.I\left(\frac{a+b}{2}, \sqrt{ab}\right)$$

ce qui donne, en utilisant l'itération de l'AGM et en gardant à l'esprit que $I(a_n,b_n) = I(a_0,b_0) = I(a,b)$, la relation

$$J(a_n,b_n) = 2J(a_{n+1},b_{n+1}) - a_nb_nI(a_{n+1},b_{n+1}) = 2J(a_{n+1},b_{n+1}) - a_nb_nI(a,b).$$

On obtient donc

$$
\begin{aligned}
(18)\qquad & 2^{n+1}\left[J(a_{n+1},b_{n+1})-a_{n+1}^2 I(a,b)\right]-2^n\left[J(a_n,b_n)-a_n^2 I(a,b)\right]\\
&=2^{n-1}\left(-4a_{n+1}^2+2a_n^2+2a_nb_n\right)I(a,b)\\
&=2^{n-1}\left(a_n^2-b_n^2\right)I(a,b).
\end{aligned}
$$

Sachant maintenant qu'en utilisant le deuxième membre de (16), on trouve

$$
\begin{aligned}
\Delta_n &= 2^n\left[a_n^2 I(a_n,b_n)-J(a_n,b_n)\right]\\
&= 2^n\int_0^{\frac{\pi}{2}}\frac{(a_n^2-b_n^2)\sin^2\theta}{\sqrt{a_n^2\cos^2\theta+b_n^2\sin^2\theta}}d\theta \leqslant 2^n(a_n^2-b_n^2)I(a_n,b_n)
\end{aligned}
$$

on a forcément $\Delta_n \to 0$ si $n\to\infty$ puisque $(a_n^2-b_n^2)\to 0$ quadratiquement. Il reste donc à sommer (18) sur $n\in\mathbb{N}$ pour obtenir (17). □

L'injection de (17) dans la relation de Legendre (17) pour $b=b'=\frac{1}{\sqrt{2}}$ donne donc

$$
I\left(1,\frac{1}{\sqrt{2}}\right)^2\left(2\left(1^2-\frac{1}{2}\sum_{k=0}^{\infty}2^k\left(a_k^2-b_k^2\right)\right)-1\right)=\frac{\pi}{2}
$$

et enfin la relation de Gauss (15) permet alors d'obtenir la remarquable formule

$$
\pi=\frac{2M\left(1,\frac{1}{\sqrt{2}}\right)^2}{1-\sum_{k=0}^{\infty}2^k\left(a_k^2-b_k^2\right)}
$$

dont l'algorithme de Brent-Salamin (8) est l'application directe.

Le peu de travail requis pour arriver à cet algorithme a longtemps fasciné les mathématiciens comme Salamin lui-même après sa découverte (qui date précisément de décembre 1973). Il semble que Gauss soit en fait parvenu à cette formule d'après son essai « Courts essais dans divers champs des mathématiques », commencé en mai 1809 [1]. Mais la complexité de sa mise en œuvre, sans algorithme efficace de multiplication et d'extraction de racines, explique sans doute que Gauss n'ait pas mesuré l'utilité de sa découverte pour le calcul des décimales de π.

Performances

Salamin montre dans [23] que si π_n est l'approximation de π après n itérations de l'algorithme (8), on a

$$
(19)\qquad |\pi-\pi_n|<\frac{\pi^2 2^{n+4}}{M\left(1,\frac{1}{\sqrt{2}}\right)^2}e^{-\pi 2^{n+1}}.
$$

Cette majoration montre que le nombre de décimales correctes de π obtenues à partir de π_n est strictement supérieur à $\left(\frac{\pi}{\log 10}\right)2^{n+1}-n\log_{10}2-2\log_{10}\left(\frac{4\pi}{M(1,1/\sqrt{2})}\right)$.

L'équipe de Kanada fut probablement la première à appliquer ce cocktail d'algorithmes (FFT, Newton, Brent-Salamin) en 1982 et en tira un peu plus de 10 millions de décimales de π.

D'autres algorithmes

À partir d'équations modulaires impliquant les fonctions thêta (dont l'algorithme de Brent-Salamin est un cas particulier), les frères Borwein ont montré que l'on pouvait construire des algorithmes convergeant à n'importe quelle vitesse (quadratique, quartique, quintique...) vers π même si la complexité des calculs augmente en conséquence. Un bon compromis semble être la formule suivante, à convergence quartique [7] :

$$\alpha_0 = 6 - 4\sqrt{2}, \qquad y_0 = \sqrt{2} - 1$$

$$y_{k+1} = \frac{1 - \sqrt[4]{1 - y_k^4}}{1 + \sqrt[4]{1 - y_k^4}}$$

$$\alpha_{k+1} = \alpha_k(1 + y_{k+1}^4) - 2^{2k+3} y_{k+1}(1 + y_{k+1} + y_{k+1}^2) \qquad \frac{1}{\alpha_k} \to \pi \tag{20}$$

Elle fut utilisée pour la première fois par Bailey puis Kanada en 1986. Bailey utilisa 12 itérations sur un *CRAY-2* pour calculer 29 360 000 décimales de π (en fait 45 millions sont possibles à cette étape). Il est amusant de constater qu'il suffit alors de moins de 100 multiplications, divisions et extractions de racines pour y parvenir !

De 1982 à 2002, ce sont toujours des formules de Ramanujan comme (5), l'algorithme de Brent-Salamin (8) ou une variante, ainsi que l'algorithme quartique des Borwein (20) qui ont été utilisés dans la course au record de calcul de décimales de π.

L'approche BBP, encore du nouveau sur π

Comment progresser ?

La multiplication, la division et l'extraction de racine s'effectuant désormais dans un temps quasi-linéaire, et sachant que l'on ne peut pas descendre en dessous d'une complexité $O(n)$, il ne faut plus guère attendre d'avancées significatives de ce côté. Nous avons vu d'autre part que des algorithmes extrêmement efficaces existaient désormais pour le calcul des décimales de π. Alors est-on condamné à voir les records tomber en fonction de la progression des performances des ordinateurs ? Oui et non !

Les mathématiques surprennent souvent là où on ne les attend plus. C'est ainsi que le 19 septembre 1995 à 0h29 (!), après des mois de recherches à tâtons, Simon Plouffe, David Bailey et Peter Borwein de Vancouver découvrent la formule apparemment simple et anodine

$$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k} \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right) \tag{21}$$

appelée depuis formule BBP. La démonstration en est presque immédiate en remarquant que $\sum_{k=0}^{\infty} \frac{1}{16^k(8k+p)} = \sqrt{2}^p \sum_{k=0}^{\infty} \int_0^{1/\sqrt{2}} x^{p-1+8k} dx = \sqrt{2}^p \int_0^{1/\sqrt{2}} \frac{x^{p-1}}{1-x^8} dx$ puis en calculant l'intégrale équivalente à (21). Euler aurait lui-même pu la découvrir. En fait, c'est à ce jour un des plus célèbres exemples de mathématiques expérimentales puisque cette formule fut découverte par l'algorithme PSLQ de

recherche de relations linéaires entre nombres. Ceci encouragea nombre d'amateurs en mathématiques à se lancer dans la recherche de telles formules grâce à PSLQ ou LLL, un algorithme similaire implémenté dans le logiciel *Pari-GP*.

Mais nos trois mathématiciens canadiens remarquent surtout que cette expression est très proche d'une décomposition en base 16 de π. Dans l'article [3] de 1996 devenu célèbre, ils montrent que l'on peut se servir de (21) pour atteindre le n-ième chiffre de π en base 2^p (*a fortiori* en base 16) sans avoir calculé les précédents, ceci en temps presque linéaire $O(n.\log^3 n)$ et en espace $O(\log n)$! ! L'espace requis étant minime, ils appliquent immédiatement ce résultat en calculant le 40 milliardième chiffre de π en base 2. La révolution est en marche.

Plouffe étend ce résultat à toutes les bases b en octobre 1996 [22] au prix d'un temps $O(n^3 \log^2 n)$ et de l'utilisation astucieuse de la série

$$\pi + 3 = \sum_{k=1}^{\infty} \frac{k.2^k (k!)^2}{(2k)!}.$$

Des améliorations en $O(n^2)$ puis en $O(n^2 \log\log n/\log^2 n)$ sont successivement proposées par Bellard en 1997 [5] puis Gourdon en 2003 [14]. De nombreuses autres formules type BBP (avec des puissances de 2 ou 3) ont depuis vu le jour pour les logarithmes d'entiers, $\zeta(3)$, $\zeta(5)$, la constante de Catalan G, et de manière générale les constantes polylogarithmiques [9, 17]. Par contre, il n'existe probablement pas de formule pour π avec une puissance de 10, autrement dit en base 10. La formule $\ln\left(\frac{9}{10}\right) = -\sum_{k=1}^{\infty} \frac{1}{10^k.k}$ montre cependant que l'on peut calculer isolément les chiffres décimaux de certaines constantes.

Ces résultats fondamentaux montrent en particulier que π appartient à la classe de complexité de Steven SC_b, regroupant les constantes dont on peut calculer les chiffres en base b en temps polynomial et espace *log*-polynomial, ce qui était auparavant jugé improbable du point de vue mémoire.

Depuis lors, Colin Percival a atteint le 10^{15}-ième chiffre binaire de π (un 0 !) au moyen d'un calcul collaboratif extravagant sur internet de 1,2 millions d'heures CPU partagées entre 1734 ordinateurs répartis dans 56 pays entre le 5 septembre 1998 et le 11 septembre 2000 !

Arrêtons-nous maintenant sur le principe de ce calcul du n-ième chiffre de π.

Atteindre le N-ième chiffre d'un nombre α sans connaître les précédents

Nous suivons ici à quelques adaptations près l'exposé remarquablement clair de Xavier Gourdon et Pascal Sebah sur le sujet [15] qui simplifiait déjà l'article original [3]. X. Gourdon est un grand connaisseur des algorithmes de calcul puisqu'il détient depuis plusieurs années le record de vitesse du calcul des décimales de π avec le programme *PiFast* (plus rapide même que le programme de l'équipe de Kanada).

Pour simplifier le propos, on se restreint à la base 2, et le N-ième bit de α désigne le N-ième bit de la partie fractionnaire de α, c'est-à-dire après la virgule. La partie fractionnaire d'un nombre x sera notée $\{x\} = x - [x]$.

Décalage

La première idée repose sur le théorème suivant

Théorème. — *Le $N+n$-ième bit de α s'obtient en calculant le n-ième bit de $2^N\alpha$ i.e. le n-ième bit de $\left\{2^N\alpha\right\}$.*

Démonstration. La décomposition en base 2 de α s'écrit

$$\alpha = [\alpha] + \{\alpha\} = \sum_{k\leqslant 0} \frac{\alpha_k}{2^k} + \sum_{k>0} \frac{\alpha_k}{2^k}, \qquad (\alpha_k \in \{0,1\})$$

d'où $\left\{2^N\alpha\right\} = \sum_{k>N} \frac{\alpha_k}{2^{k-N}} = \sum_{k>0} \frac{\alpha_{N+k}}{2^k}$. Le n-ième bit de $\left\{2^N\alpha\right\}$ est donc α_{N+n} qui est bien le $N+n$-ième bit de α. □

Exemple. — Cherchons le 13ième bit de π. Comme on a $2^{12}\pi = 12867.9635...$, en particulier, $\left\{2^{12}\pi\right\} = 0.9635....$ Il reste donc à calculer le 1er bit de 0.9635. En passant en binaire, on a

$$0.9635... = \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \frac{0}{2^5} + \frac{1}{2^6} + \frac{1}{2^7} + ... = [0.1111011...]_{base\ 2}$$

donc le 13ième bit de π est 1, et le 17ème bit est 0.

Chercher le $N+1$-ième bit de π correspond donc à trouver le premier bit de $\left\{2^N\pi\right\}$. D'après la formule BBP (21), cela correspond au premier bit de la série

$$\pi_N = \sum_{n=0}^{\infty} \left(\left\{ \frac{4.2^{N-4n}}{8n+1} \right\} - \left\{ \frac{2.2^{N-4n}}{8n+4} \right\} - \left\{ \frac{2^{N-4n}}{8n+5} \right\} - \left\{ \frac{2^{N-4n}}{8n+6} \right\} \right) = A_N + B_N$$

où A_N et B_N sont les sommes

$$A_N = \sum_{0\leqslant n\leqslant N/4}, \qquad B_N = \sum_{n>N/4}. \tag{22}$$

Compte tenu de la décroissance rapide de 2^{N-4n} pour $n > \frac{N}{4}$, il suffit d'évaluer seulement les premiers termes de B_N (en virgule flottante !), plus exactement suffisamment pour que le reste de la somme soit inférieur à la précision requise (ici 1 bit après la virgule).

Concernant A_N, on peut mettre son terme général sous la forme

$$\left\{ \frac{p.2^n}{m} \right\}$$

avec p, n et m dans $\mathbb{N}$. En écrivant $p.2^n = qm + r$ la division euclidienne de $p.2^n$ par m, on voit que comme $r < m$, $\left\{ \frac{p.2^n}{m} \right\} = \frac{r}{m}$. Ceci s'écrit encore

$$\left\{ \frac{p.2^n}{m} \right\} = \frac{p.2^n \pmod m}{m}.$$

Exponentiation

Imaginons ainsi que l'on veuille calculer le 1000ème bit de $\frac{1}{2^{35}49}$. Grâce aux principes précédents, cela revient à calculer le 965ème bit de $\frac{1}{49}$ et donc le 1er bit de $\frac{2^{964}}{49}$. En vertu de (23), il faut alors trouver r tel que $2^{964} = 49q + r$ donc évaluer $2^{964} \pmod{49}$.

Le calcul de $2^{964} \pmod{49}$ s'effectue au moyen de la méthode appelée exponentiation binaire ("binary powering" ou "binary exponentiation"), dont l'idée semble avoir été utilisée dès 200 avant J.C [18], et même envisagée par les Égyptiens pour effectuer la multiplication ! Cela revient simplement à utiliser l'arithmétique modulo 49, autrement dit à se placer dans $\mathbb{Z}/49\mathbb{Z}$, en trois étapes.

(1) On décompose 964 en puissances de 2 : $989 = 512 + 256 + 128 + 64 + 4$.
(2) On calcule de proche en proche chaque puissance de 2 jusqu'à 512 :

$$\begin{array}{ll}
2^2 = 4; & 2^4 = \left(2^2\right)^2 = 4 * 4 = 16; \\
2^8 = 16^2 = 256 = 49 * 5 + 11 = 11; & 2^{16} = 11^2 = 121 = 23; \\
2^{32} = 23^2 = 529 = 39; & 2^{64} = 39^2 = 1521 = 2; \\
2^{128} = 2^2 = 4; & 2^{256} = 16; \\
2^{512} = 16^2 = 11. &
\end{array}$$

(3) On utilise les étapes 1 et 2 :

$$2^{964} = 2^{512+256+128+64+4} = 11 \times 16 \times 4 \times 2 \times 4 = 5632 = 46.$$

Pour obtenir plus généralement $r = p.2^n \pmod{m}$, on initialise r à 1 et on prend t la plus grande puissance de 2 inférieure à n. Puis on applique l'algorithme suivant équivalent à notre exemple :

(1) si $n \geqslant t$, alors $r = 2.r \pmod{m}$; $n = n - t$; FinSi
(2) $t = t/2$;
(3) si $t \geqslant 1$ alors $r = r^2 \pmod{m}$; aller à l'étape 1 ; FinSi.

Enfin on termine par $r = p.r \pmod{m}$; pour prendre en compte p. En raison de la décomposition de n en puissance de 2, on utilise $O(\log n) \pmod{m}$ opérations pour ce calcul, ce qui est très faible !

Étapes finales

Il reste à obtenir $\frac{r}{m} = \frac{p.2^n \pmod{m}}{m}$ et à sommer le tout sur $0 \leqslant n \leqslant \frac{N}{4}$ pour obtenir A_N dans (22). Il faut ici remarquer que si le calcul de chaque terme de A_N est effectué en virgule flottante et que, disons, le dernier bit est erroné, alors au pire la propagation des retenues sur toute la somme produira une erreur sur $1 + \log_2 \frac{N}{4}$ bits. Pour des valeurs de N non extravagantes, on pourra donc mener les calculs de $\frac{r}{m}$ en toute sérénité avec une précision arithmétique de 64 bits seulement.

Pour cette raison et en remarquant que pour A_N, on somme $O(N)$ termes nécessitant chacun $O(\log N)$ opérations grâce à l'exponentiation, l'algorithme requiert $O(N.\log N.M(\log N))$ opérations et $O(\log N)$ en espace, où $j < M(j) \leqslant j^2$ est la complexité de la multiplication de deux entiers de taille j bits.

Une formule pleine de ressources

L'accès presque direct aux chiffres de ces constantes a fait naître chez les mathématiciens l'idée que l'on pourrait trouver des propriétés de répartition de ces digits, et que l'on était peut-être proche d'une preuve de la normalité de π (et donc de l'irrationnalité de la constante de Catalan G ou des ζ impairs). La normalité d'un nombre requiert que chaque n-uplet possible apparaisse avec la probabilité $\frac{1}{b^n}$ dans les digits en base b de ce nombre. En octobre 2000, Bailey et Crandall ont réduit cette condition de normalité à la vérification de l'hypothèse suivante :

Conjecture. — *Soit* $r_n = \frac{p(n)}{q(n)} \in \mathbb{Q}(n)$, $n > 0$, *avec* $\deg p < \deg q$ *et* r_n *sans pôles sur* $\mathbb{N}$ *(c'est la partie polynomiale des formules BBP). Soit une base* $b \geqslant 2$ *et* $x_0 = 0$. *Alors la suite* $(x_n)_{n\in\mathbb{N}}$ *définie par*

$$x_n = (b.x_{n-1} + r_n) \pmod 1$$

n'a qu'un nombre fini de valeurs d'adhérence ou bien est équidistribuée sur $[0, 1]$.

Cette forme de suite est équivalente à la représentation BBP d'une constante puisque si $\alpha = \sum_{k=1}^{\infty} \frac{1}{b^k} r(k)$, alors $\{b^n\alpha\} = (x_n + t_n) \mod 1$ où

$$t_n = \sum_{k=1}^{\infty} \frac{1}{b^k} r(k+n)$$

tend vers 0 si $n \to \infty$ puisque $\deg p < \deg q$.

En outre, la suite $(\{b^n\alpha\})$ a un nombre fini de valeurs d'adhérence uniquement si α est rationnel [4].

La notion d'équidistribution est vérifiée si la proportion d'apparition d'une séquence à valeurs dans $[0, 1]$ dans un intervalle donné $[c, d]$ est justement la longueur de cet intervalle, bref si les valeurs prises sont distribuées uniformément dans $[0, 1]$. $(x_n)_{n\in\mathbb{N}}$ est équidistribuée si

$$\lim_{n\to\infty} \frac{Card\,\{x_j \in [c, d],\ j < n\}}{n} = d - c.$$

L'équidistribution pour ce type de suites implique la normalité [19]. Compte tenu de la variété des constantes impliquées dans des représentations BBP, on touche là à des avancées importantes, notamment pour les ζ impairs. Il est amusant de voir la simplicité de la formule BBP dont sont tirées toutes ces conséquences. On consultera [4, 20] pour approfondir ces questions ouvertes.

Une quête sans fin ?

Record en date

Le 6 décembre 2002, Kanada, compétiteur infatigable qui détient ou reprend le record de calcul de décimales de π depuis plus de 20 ans, a calculé 1 241 100 000 000 décimales de π. La surprise est venue du fait qu'il a utilisé cette fois deux formules de type Machin comme l'eq. (4).

Ce retour à des formules étonnament simples après l'utilisation pendant une quinzaine d'années des algorithmes de Brent-Salamin, des Borwein ou des séries de Ramanujan et Chudnovsky était vraiment inattendu. Il semble que l'utilisation perpétuelle de racines, multiplications et divisions nécessitait l'utilisation de

la transformée de Fourier rapide (FFT) à très grande échelle. Cette dernière requiert énormément de mémoire pour fonctionner. Kanada est donc revenu à des méthodes plus sages comme les formules type Machin, qui nécessitent sensiblement plus d'opérations arithmétiques mais moins de FFT et donc beaucoup moins de mémoire. Kanada estime que son implémentation est environ deux fois plus plus rapide que la précédente qui utilisait l'algorithme (8) de Brent-Salamin et celui d'ordre quartique des Borwein (éq. 20). Les calculs ont été effectués en base hexadécimale, soit 1 030 700 000 000 digits. Les formules employées sont :

$$\pi = 48 \arctan \frac{1}{49} + 128 \arctan \frac{1}{57} - 20 \arctan \frac{1}{239} + 48 \arctan \frac{1}{110443} \tag{23}$$

$$\pi = 176 \arctan \frac{1}{57} + 28 \arctan \frac{1}{239} - 48 \arctan \frac{1}{682} + 96 \arctan \frac{1}{12943}. \tag{24}$$

La première a été trouvée en 1982 par un professeur de mathématiques et compositeur, Takano, et la seconde est une découverte de Störmer en 1896.

Ce calcul de Kanada recèle une seconde originalité : comme le résultat avait été obtenu en base 16, après avoir vérifié l'adéquation entre les deux calculs, il a effectué une vérification supplémentaire en calculant directement les 20 digits hexadécimaux à la position 1 000 000 000 001 à l'aide de l'approche par formules BBP présentée précédemment. Le résultat B4466E8D21 5388C4E014, qui a requis 21 heures de travail, a parfaitement correspondu aux calculs effectués à l'aide des formules d'arctan. Les digits hexadécimaux ont alors été convertis en base dix, une opération peu triviale d'ailleurs, reconvertis en hexadecimal pour vérification, puis le record a été officialisé [2].

Les calculs (tout compris) ont duré près de 600 heures sur un HITACHI SR8000/MP doté de 1TB de stockage (1024Go), soit la même mémoire que pour son précédent record de 1999, alors que 6 fois plus de décimales ont été calculées !

Perspectives et motivations

Comment expliquer que la course aux décimales reste d'actualité ? Les motivations pour battre le record de décimales de π n'ont en fait jamais manquées, confinant même parfois à un soupçon de mauvaise foi. On citera pêle-mêle le test des ordinateurs (un bug aurait été découvert par Bailey lors de son record de calcul en 1986 sur des *Cray-2*), l'hypothétique apparition d'irrégularités dans la répartition des décimales calculées (chou blanc de ce côté pour l'instant) ou la mise au point de techniques toujours plus efficaces d'implémentation de calcul des décimales (la compétition fait actuellement rage sur l'internet entre plusieurs mathématiciens informaticiens pour le titre de programme le plus rapide du monde).

Chacune de ces raisons prise séparément n'est pas suffisante. Il serait probablement plus honnête de dire que c'est la conjonction de toutes ces raisons, sans compter la passion engendrée par la « personnalité » de π, qui alimente et renouvelle la compétition. Il est vrai que l'implémentation moderne des librairies d'arithmétiques sur grands nombres (reposant sur les techniques de FFT, de Newton vues précédemment) doit beaucoup à la course aux décimales de π. Il est vrai également que la mise au point de programmes efficaces n'est pas à la portée de n'importe qui et qu'il faut soigneusement connaître l'architecture de son calculateur pour espérer obtenir une performance intéressante. C'est un challenge pour de

nombreux informaticiens doués en maths (ou l'inverse !). Nous avons vu aussi que la découverte récente de la formule BBP (21) avait ouvert un champ d'investigations théorique immense.

J'ajouterai que la popularité de π joue un rôle primordial : il est ainsi une justification peut-être rarement avancée mais qui prend tout son sens auprès des simples amateurs de mathématiques membres de la secte des adorateurs de π, ou même visible en écumant les forums de mathématiques de par le monde : la théorie des nombres, l'analyse classique et les constantes ont une base accessible, au moins en apparence, pour les non-mathématiciens et restent les plus grands fournisseurs de petits exercices et de propriétés amusantes des nombres. C'est par ce biais que naissent beaucoup de vocations de mathématiciens, et il suffit de consulter les pages web de mathématiciens comme Bailey, Plouffe, Kanada ou des frères Borwein pour se convaincre qu'ils gardent à cinquante ans passés une passion rafraîchissante pour les constantes, parties visibles de l'iceberg mathématique. La difficulté d'abstraction de certains autres domaines des mathématiques comme la géométrie algébrique les confine probablement à un public davantage connaisseur et ils ne bénéficient donc pas d'autant d'ambassadeurs comme π ou les nombres premiers peuvent l'être en théorie des nombres. Il faut ainsi noter que la quête du plus grand nombre de Mersenne premier est un exercice très à la mode actuellement.

Mais laissons le mot de la fin à Genuys à qui on demandait, après son record à 10 000 décimales en 1958, pourquoi il avait choisi π et qui répondit tout simplement : « C'était pour moi un exercice de programmation, j'aurais pu choisir un autre nombre mais e c'était trop facile et c (la constante d'Euler) trop difficile ! Et puis il y avait le record ! » [21].

Références

[1] J. Arndt, C. Haenel, "π Unleashed", Springer-Verlag, Berlin Heidelberg New York, 2001.

[2] D. H. Bailey, « Some Background on Kanada's Recent Pi Calculation", may 2003, preprint, http ://www.nersc.gov/~dhbailey/dhbpapers/dhb-kanada.pdf.

[3] D.H. Bailey, P.B. Borwein, S. Plouffe, « On the Rapid Computation of Various Polylogarithmic Constants", Mathematics of Computation, 1997, vol. 66, pp. 903-913.

[4] D. H. Bailey, R. E. Crandall, "On the Random Character of Fundamental Constant Expansions", Experimental Mathematics, 2001, vol. 10, n° 2, pp. 175-190.

[5] F. Bellard, "Computation of the n'th digit of pi in any base in $O(n^2)$, unpublished, 1997, http ://fabrice.bellard.free.fr/pi/pi_n2.ps.

[6] L. Berggren, J. Borwein, P. Borwein, "Pi : A Source Book", Springer-Verlag, 2nd ed., 1997.

[7] J. Borwein, P. Borwein, "PI and the AGM : A Study in Analytic Number Theory and Computational Complexity", Wiley, 1987.

[8] R. Brent, "Fast multiple-precision evaluation of elementary fonctions", Journal of the Association of Computing Machinery, 1976, pp.242-251.

[9] D. J. Broadhurst, "Polylogarithmic ladders, hypergeometric series and the ten millionth digits of z(3) and z(5)", 1998, preprint.

[10] S. A. Cook, S. O. Aanderaa, "On the minimum computation of functions", Trans. AMS, 1969, vol. 142, pp291-314.

[11] J. W. Cooley, J. W. Tukey, "An algorithm for the machine calculation of complex Fourier series", Math. Comp. 1965, vol 19, pp. 297-301.

[12] J.-P. Delahaye, "Le Fascinant Nombre π", Bibliothèque Pour La Science, Belin, 1997.

[13] P. Eymard, J.-P. Lafon, "Autour du Nombre π", Hermann, Paris, 1999.

[14] X. Gourdon, "Computation of the n-th decimal digit of π with low memory", preprint, 2003, http ://numbers.computation.free.fr/Constants/Algorithms/nthdecimaldigit.pdf.

[15] X. Gourdon, P. Sebah, "N-th digit computation", preprint, 2003, http ://numbers.computation.free.fr/Constants/Algorithms/nthdigit.pdf.

[16] M. D. Householder, "The Numerical Treatment of a Single Nonlinear Equation", 1970, MacGraw-Hill, New-York.
[17] G. Huvent, "Formules BBP", 2001, Preprint. `http://ano.univ-lille1.fr/seminaries/expo\_huvent01.pdf`.
[18] D. E. Knuth, "The Art of Computer Programming. Vol. 2 : Seminumerical Algorithms", Addison-Wesley, Reading, MA, 1981.
[19] L. Kuipers and H.Niederreiter, "Uniform distribution of sequences", Wiley-Interscience, New York, 1974.
[20] J. C. Lagarias, "On the normality of fundamental constants", Experiment. Math., 2001, vol. 10, n° 2.
[21] "Le nombre π", Le Petit Archimède, Association pour le Dévelopement de la Culture Scientifique, Amiens, 1980.
[22] S. Plouffe, "On the computation of the n-th decimal digit of various transcendental numbers", unpublished, 11/1996.
[23] E. Salamin, "Computation of π using arithmetic-geometric mean", Mathematics of computation, 1976, vol. 30, pp. 565-570.
[24] A. Schönhage, V. Strassen, "Schennelle Multiplikation grosser Zahlen", Computing, 1971, vol. 7, pp. 281-292.
[25] J. Tropfke, "Geschichte der Elementarmathematik", Vierter Band, Ebene Geometrie, Dritte Auflage, Walter De Gruyter & Co, 1940.