FORMULES à la MACHIN

Raymond SEROUL

1. Introduction.

La chasse aux décimales du nombre π n'a vraiment pris son essor qu'à partir du moment où l'on a disposé de formulles telles que :

$$\begin{aligned}
\pi/4 &= 4\,\mathrm{Arctg}\,(1/5) - \mathrm{Arctg}\,(1/239) && \text{(John MACHIN 1706)}\\
&= \mathrm{Arctg}\,(1/2) + \mathrm{Arctg}\,(1/3) && \text{(HUTTON 1776)}\\
&= 2\,\mathrm{Arctg}\,(1/3) + \mathrm{Arctg}\,(1/7) && \text{(CLAUSEN 1847)}\\
&= \mathrm{Arctg}\,(1/2) + \mathrm{Arctg}\,(1/5) + \mathrm{Arctg}\,(1/8) && \text{(DASE 1884)}
\end{aligned}$$

En 1974 (*), on a calculé un million de décimales de π en utilisant la formule suivante (GAUSS)

$$\pi/4 = 12\,\mathrm{Arctg}\,(1/18) + 8\,\mathrm{Arctg}\,(1/57) - 5\,\mathrm{Arctg}\,(1/239).$$

Ce calcul a ensuite été vérifié à l'aide de la formule dûe à STÖRMER (1896)

$$\pi/4 = 6\,\mathrm{Arctg}\,(1/8) + 2\,\mathrm{Arctg}\,(1/57) + \mathrm{Arctg}\,(1/239).$$

Sachant que pour $x > 0$ on a l'égalité

$$\mathrm{Arctg}\,(1/x) = \pi/2 - \mathrm{Arctg}\,(x) = 2\,\mathrm{Arctg}\,(1) - \mathrm{Arctg}\,(x),$$

les formules précédentes se réécrivent sous la forme plus sympathique

$$\begin{aligned}
\mathrm{Arctg}\,(3) &= 3\,\mathrm{Arctg}\,(1) - \mathrm{Arctg}\,(2) && \text{(HUTTON)}\\
\mathrm{Arctg}\,(7) &= \mathrm{Arctg}\,(1) + 2\,\mathrm{Arctg}\,(2) && \text{(CLAUSEN)}\\
\mathrm{Arctg}\,(8) &= 5\,\mathrm{Arctg}\,(1) - 2\,\mathrm{Arctg}\,(2) - \mathrm{Arctg}\,(5) && \text{(DASE)}\\
\mathrm{Arctg}\,(239) &= -5\,\mathrm{Arctg}\,(1) + 4\,\mathrm{Arctg}\,(5) && \text{(MACHIN)}\\
&= 17\,\mathrm{Arctg}\,(1) - 6\,\mathrm{Arctg}\,(8) - 2\,\mathrm{Arctg}\,(57) && \text{(STÖRMER).}
\end{aligned}$$

(*) En 1979, il était question d'un projet de calcul avec 20 millions de chiffres binaires. Mais la technique de calcul est désormais basée sur un autre concept (formule de BRENT-SALAMIN).

En l'honneur du premier découvreur d'une telle formule, appelons formule *à la* MACHIN une égalité de la forme :

$$\text{(M)} \qquad \text{Arctg}\,(n) = c_1\text{Arctg}\,(1) + c_2\text{Arctg}\,(2) + \cdots + c_{n-1}\text{Arctg}\,(n-1)$$

où les c_i sont des entiers.

Remarque : la formule de GAUSS

$$\text{Arctg}\,(239) = -39/5\text{Arctg}\,(1) + 12/5\,\text{Arctg}\,(18) + 8/5\,\text{Arctg}\,(57)$$

n'est pas une formule *à la* MACHIN selon notre définition, car les c_i n'y sont pas entiers.

Lorsqu'il est possible de trouver une formule *à la* MACHIN pour l'entier n, on dit que n est décomposable. La caractérisation de ces entiers a été obtenue en 1949 par John TODD :

Théorème 1. — *Un entier $n \leq 2$ est décomposable si et seulement s'il vérifie la condition* (T) *suivante : tout diviseur premier de $1 + n^2$ est aussi un diviseur d'un entier de la forme $1 + d^2$, avec $0 < d < n$.*

Les premiers entiers décomposables sont donc 3, 7, 8, 13, 18, 21, 30, ...

En outre, J.TODD est capable de fabriquer, pour chaque entier décomposable, une formule *à la* MACHIN. C'est ce travail que je me propose d'exposer ici. (On trouvera une liste des 30 premières formules *à la* MACHIN à la fin de cet article.)

2. La condition (T) est nécessaire.

Soit $n \geq 2$ un entier décomposable et qui vérifie donc (M). Posons

$$[1+i]^{c_1}[1+2i]^{c_2}\ldots[1+(n-1)i]^{c_{n-1}} = [a+ib]/[u+iv]$$

($a+bi$ recueille les facteurs correspondants à $c_k > 0$ et $u+vi$ ceux correspondant à $c_k < 0$). L'idée de base, déjà connue de GAUSS, consiste à remarquer que l'argument de $1+in$ est précisément $\text{Arctg}\,(n)$. Par conséquent, les nombres complexes $1+in$ et $[a+ib]/[u+iv]$ ont même argument. Aussi leur quotient

$$[a+ib]/[u+iv][1+in] = [A+iB]/[u^2+v^2][1+n^2]$$

est-il un nombre réel. Cela exige $B = 0$, d'où $A = (au+bv)(1+n^2)$. On a donc

$$[a+ib]/[u+iv][1+in] = [au+bv]/[u^2+v^2]$$

soit encore

$$[u^2+v^2][a+bi] = [au+bv][u+vi][1+ni].$$

En passant aux modules, on trouve $[u^2+v^2][a^2+b^2] = [au+bv]^2[1+n^2]$, ce qui donne

$$[1+1^2]^{|c_1|}[1+2^2]^{|c_2|}\dots[1+(n-1)^2]^{|c_{n-1}|}=a^2[1+n^2].$$

La condition (T) est ainsi vérifiée.

3. L'anneau $\mathbf{Z}[i]$ des entiers de GAUSS.

Il nous faut maintenant faire plus ample connaissance avec les nombres complexes de la forme $x+iy$ avec $x,y\in\mathbf{Z}$. On note cet ensemble $\mathbf{Z}[i]$. Il s'agit manifestement d'un anneau commutatif et intègre, appelé anneau des entiers de GAUSS en hommage à leur créateur qui les introduisit vers 1830.

Si $\alpha=x+iy$ est un entier de GAUSS, on pose

$$N(\alpha)=|\alpha|^2=x^2+y^2$$

et on dit que $N(\alpha)$ est la *norme* de α (à ne pas confondre avec la *norme euclidienne* qui est aussi le module de α). Il est clair que $N(\alpha\beta)=N(\alpha)\ N(\beta)$.

Pour mieux illustrer les propriétés de $\mathbf{Z}[i]$, nous allons les mettre en parallèle avec les propriétés correspondantes et bien connues des anneaux $\mathbf{Z}$ et $\mathbf{R}[X]$ (polynômes à coefficients réels).

Tout d'abord, on dit que e est une *unité* d'un anneau A s'il existe $e'\in A$ tel que l'on ait $ee'=1$. Les unités de $\mathbf{Z}$ sont donc les entiers 1 et -1. Quant à celles de $\mathbf{R}[X]$, ce sont les polynômes réduits à une constante non nulle.

Si ϵ est une unité de $\mathbf{Z}[i]$, on aura $\epsilon\epsilon'=1$ d'où $N(\epsilon)N(\epsilon')=1$. On déduit immédiatement de cela que les unités de $\mathbf{Z}[i]$ sont caractérisées par la condition $N(\epsilon)=1$ et que ce sont les entiers de GAUSS 1, -1, i, $-i$.
Lorsque l'on a $\alpha=\beta\epsilon$, avec ϵ unité, on dit que α et β sont *associés*. Les associés de $x+iy$ sont donc $\pm(x=iy)$ et $\pm(y-ix)$.

Soient a,b deux éléments de $\mathbf{Z}$, avec $b\neq 0$. On sait qu'il existe des entiers q et r vérifiant $a=bq+r$ et $|r|<|b|$. De même, si $a(X)$ et $b(X)$ sont deux polynômes, avec degré $b(X)>0$, on sait trouver deux polynômes $q(X)$ et $r(X)$ tels que $a(X)=b(X)\ q(X)+r(X)$ et degré $r(X)<$ degré $b(X)$. On dit que les anneaux $\mathbf{Z}$ et $\mathbf{R}[X]$ sont munis d'une *division euclidienne.*

Nous allons constater qu'un phénomène analogue se produit dans $\mathbf{Z}[i]$.
Soient α et β deux entiers de GAUSS, avec $\beta\neq 0$. Posons $x+iy=\alpha/\beta$ puis $\gamma=\mathrm{E}(x)+i\,\mathrm{E}(y)$ (parties entières, x et y ne sont que rationnels ici). Il est immédiat que l'on a

$$\alpha=\beta\gamma+\rho\quad\text{et}\quad N(\rho)<N(\beta).$$

Cela montre que l'anneau $\mathbf{Z}[i]$ est, lui aussi, muni d'une division euclidienne. (L'analogue de la fonction norme est la valeur absolue dans le cas de $\mathbf{Z}$ et le degré dans celui de $\mathbf{R}[X]$.)

Lorsque l'on dispose d'un anneau euclidien, on peut y faire de l'arithmétique comme dans $\mathbf{Z}$. La notion qui correspond à celle de nombre premier est celle

d'élément *irréductible*. En utilisant la division euclidienne, on démontre comme on le fait pour $\mathbf{Z}$, que tout élément est un produit de facteurs irréductibles, et que cette décomposition est unique. Par exemple, on sait que tout polynôme non constant de $\mathbf{R}[X]$ est un produit de polynômes du premier degré et de polynômes du second degré n'ayant pas de racines réelles.

Voyons alors ce que donne cette théorie des anneaux euclidiens pour $\mathbf{Z}[i]$.

Théorème 2. — *Un entier de GAUSS est irréductible si et seulement si l'un de ses associés fait partie de la liste suivante*

(a) $1+i$,

(b) $a+bi$, *où* a^2+b^2 *est un nombre premier de* $\mathbf{Z}$ *de la forme* $4n+1$,

(c) p, *où* p *est un nombre premier de* $\mathbf{Z}$ *de la forme* $4n+3$.

Commentaires :

1) Un irréductible du type (b) est $5+42i$ puisque $1789 = 5^2+42^2$. Un irréductible du type (c) est 1979.

2) Si ω est un irréductible du type (a), sa norme est égale à 2. S'il est du type (b), sa norme $N(\omega)$ est un nombre premier de la forme $4n+1$. Si ω est du type (c), $N(\omega)$ est le carré d'un nombre premier de la forme $4n+3$. Le calcul de la norme d'un entier de GAUSS permet donc de tester facilement si l'on a affaire à un irréductible.

3) Les unités ± 1, $\pm i$ ne sont pas irréductibles par définition (1 n'est pas premier dans $\mathbf{Z}$).

4) Si $p \in \mathbf{Z}$ est un nombre premier (dans $\mathbf{Z}$), il n'est pas forcément irréductible dans $\mathbf{Z}[i]$. C'est précisément tout l'intérêt des entiers de GAUSS que d'arriver à faire "éclater" en produits de facteurs certains nombres premiers. C'est aussi pour cette raison que l'on préfère utiliser la terminologie "élément irréductible".

Voici deux exemples de décomposition en facteurs irréductibles

$5 = (1+2i)(1-2i) = (2+i)(2-i)$ et $1+57i = -(1+i)(1+2i)^3(3+2i)$.

On remarquera que nous avons donné deux décompositions de 5. Mais ces deux factorisations sont étroitement liées, car $2+i = i(1-2i)$ et $2-i = -i(1+2i)$.

Plus généralement, si $\xi = \omega_1 \ldots \omega_n$ est une décomposition de ξ en facteurs irréductibles, toutes les autres décompositions de ξ sont, à l'ordre près des facteurs, de la forme $\xi = \epsilon_1\omega_1 \ldots \epsilon_n\omega_n$, avec $\epsilon_1 \ldots \epsilon_n = 1$. C'est en ce sens que l'on parle de l'*unicité* de la décomposition en facteurs irréductibles.

6) Soit p un nombre premier de la forme $4n+1$. Peut-on avoir *deux* décompositions de p en une somme de deux carrés? Supposons que l'on ait $p = a^2+b^2 = c^2+d^2$, avec $a+ib$ irréductible. De l'égalité $(a+ib)(a-ib) = (c+id)(c-id)$, on déduit (quitte à changer d en $-d$) que $a+ib$ divise $c+id$. Nous avons donc $c+id = \epsilon(a+ib)$, puis, en passant aux normes, $p = N(\epsilon)p$. Ceci montre que ϵ est une unité. Autrement dit, la décomposition de p est unique et la liste des irréductibles de norme p est formée des huit entiers de GAUSS $\pm a \pm bi$ et $\pm b \pm ai$.

4. La condition (T) est suffisante.

4.1. Présentation de l'algorithme.

Soit $n \geq 2$ un entier qui vérifie la condition (T). L'idée de TODD est la suivante : il construit un algorithme qui détermine un entier $M \geq 1$ ainsi que des entiers w_i satisfaisant les conditions $|w_i| < n$ et

$$M(1+in) = \epsilon(1+iw_1)(1+iw_2)\dots(1+iw_t) \qquad (\epsilon \text{ unité}).$$

La comparaison des arguments fournit immédiatement une formule *à la* MACHIN. Soyons plus précis et considérons l'entier $n = 342$. Décomposons tout d'abord $1+342i$ en facteurs irréductibles

$$1+342i = (1+2i)(7+10i)(11-6i).$$

Choisissons un facteur irréductible qui ne soit pas de la forme $\pm 1 \pm wi$ ou $w \pm i$, par exemple $7+10i$. Nous avons l'égalité

$$(7+10i)(3+2i) = 1+44i.$$

Multiplions $1+342i$ par $(3+2i)(3-2i) = 13$, ce qui donne

$$13(1+342i) = (1+2i)(1+44i)(3-2i)(11-6i).$$

Réitérons ces opérations tant qu'il reste un facteur qui ne soit pas de la forme $\pm 1 + wi$ ou $w \pm i$. Nous obtenons par exemple

$$\begin{cases} (3-2i)(1-i) = 1-5i & (1-i)(1+i) = 2 \\ 2.13\,(1+342i) = (1+2i)(1+44i)(1-5i)(1+i)(11-6i) \end{cases}$$

$$\begin{cases} (11-6i)(5-9i) = 1-129i & (5-9i)(5+9i) = 106 \\ 2.13.106\,(1+342i) = (1+2i)(1+44i)(1-5i)(1+i)(1-129i)(5+9i) \end{cases}$$

$$\begin{cases} (5+9i)(2+1) = 1+23i & (2+i)(2-i) = 5 \\ 2.13.106.5\,(1+342i) = (1+2i)(1+44i)(1-5i)(1+i) \\ \qquad\qquad (1-129i)(1+23i)(2-i)\,. \end{cases}$$

Tous calculs effectués, il vient

$$2.5.13.106\,(1+342i) = -i(1+2i)(1+44i)(1-5i)(1+i) \\ (1-129i)(1+23i)(1+2i).$$

La comparaison des arguments montre que l'on a

$$\operatorname{Arctg}(342) = k\operatorname{Arctg}(1) + 2\operatorname{Arctg}(2) - \operatorname{Arctg}(5) \\ +\operatorname{Arctg}(23) + \operatorname{Arctg}(44) - \operatorname{Arctg}(129)$$

(où k est un entier convenable). On termine en calculant

$$k = \Big[\text{Arctg}\,(342) - 2\,\text{Arctg}\,(2) + \text{Arctg}\,(5) \\ -\text{Arctg}\,(23) - \text{Arctg}\,(44)\Big]/\text{Arctg}\,(1)$$
$$= -1.$$

L'algorithme de TODD fournit ainsi la formule *à la* MACHIN

$$\text{Arctg}\,(342) = -\text{Arctg}\,(1) + 2\,\text{Arctg}\,(2) - \text{Arctg}\,(5) \\ + \text{Arctg}\,(23) + \text{Arctg}\,(44) - \text{Arctg}\,(129).$$

Remarquons en passant que l'on peut obtenir une nouvelle formule. En effet, 129 est décomposable, soit

$$\text{Arctg}\,(129) = 2\text{Arctg}\,(1) + \text{Arctg}\,(23) - \text{Arctg}\,(28).$$

D'où la nouvelle formule

$$\text{Arctg}\,(342) = -3\,\text{Arctg}\,(1) + 2\,\text{Arctg}\,(2) - \text{Arctg}\,(5) \\ + \text{Arctg}\,(28) + \text{Arctg}\,(44).$$

4.2. Comment se fabrique une égalité du type $(7 + 10i)(3 + 2i) = 1 + 44i$.

Lemme 3. — *Soit $p = u^2 + v^2$ un nombre premier de la forme $4k + 1$. Il existe un unique entier de* GAUSS *$x + iy$ tel que l'on ait*

$$(u + iv)(x + iy) = 1 + iw, \quad |w| < p/2 \quad \textit{et} \quad N(x + iy) < N(u + iv)/3.$$

En outre, si p divise $1 + d^2$, on a $|w| \leq d$.

Démonstration : considérons l'ensemble W des w qui figurent dans les égalités $(u + iv)(x + iy) = 1 + iw$. En séparant parties réelle et imaginaire, nous obtenons le système

$$ux - vy = 1, \quad vx + uy = w.$$

Puisque u et v sont premiers entre eux, il existe x_0 et y_0 tels que $ux_0 - vy_0 = 1$ (BEZOUT). La résolution de l'équation $ux - vy = 1$ montre que l'on a $x = x_0 + kv$, $y = y_0 + ku$ (k entier arbitraire) d'où l'on déduit $w = m + kp$ avec $m = vx_0 + uy_0$. Par conséquent, il existe une valeur de k et une seule telle que $|w| < p/2$. Nous avons ensuite

$$\begin{aligned} N(x + iy) &= N(1 + iw)/N(u + iv) = (1 + w^2)/p \\ &< (1 + p^2/4)/p \\ &< p/3 \qquad (\text{car } p \geq 5). \end{aligned}$$

Supposons maintenant que p divise $1+d^2$. Puisque w est le plus petit élément, en valeur absolue, de W il nous suffira de prouver que $\pm d \in W$ pour démontrer $|w| \leq d$. L'égalité

$$(u+vd)(u-vd) = u^2+v^2-(1+d^2)v^2 = p-(1+d^2)v^2$$

montre que p divise $(u+vd)(u-vd)$. Comme p est premier, cela exige que p divise $u+tv$, avec $t = \pm d$. Ecrivons ensuite

$$(1+it)/(u+iv) = (1+it)(u-iv)/p = (u+tv)/p + i(tu-v)/p.$$

Nous savons déjà que $x = (u+tv)/p$ est un entier. Montrons qu'il en est de même de $y = (tu-v)/p$. L'égalité $t(tu-v) = u(1+t^2)-(u+tv)$ prouve que p divise t ou $tu-v$. Mais p vivise $1+t^2 = 1+d^2$: il ne peut donc pas diviser t. Cela démontre que $x+iy$ est un entier de GAUSS, soit encore $t \in W$.

Exemple : $u+iv = 7+10i$ donne $x_0 = 3, y_0 = 2, w = 44+kp, p = N(u+iv) = 144$. La plus petite valeur de w est obtenue pour $k = 0$, ce qui donne $(7+10i)(3+2i) = 1+44i$.

4.3. L'algorithme de TODD.

Entrée : un entier $n \geq 2$.

Sortie : si l'entier n ne vérifie pas la condition (T), l'algorithme l'annonce. Sinon, l'algorithme écrit des entiers de GAUSS $1+iw_1, \ldots, 1+iw_r$, avec $|w_i| < n$, puis termine en écrivant une unité ϵ et un entier M qui vérifient

$$M(1+in) = \epsilon(1+iw_1)\ldots(1+iw_r).$$

Preuve de cet algorithme.

Supposons tout d'abord que l'entier n vérifie la condition (T). Les propriétés suivantes restent alors constamment vérifiées.

(T_1) *W est un produit d'entiers de* GAUSS *de la forme* $1+iw$, *avec* $|w| < n$,

(T_2) *α est un entier de* GAUSS. *Si ξ est un facteur irréductible de α, il est du type (a) ou (b), et $N(\xi)$, qui est un nombre premier, divise un entier de la forme* $1+d^2$ *avec* $0 < d < n$,

(T_3) *M est un entier (ordinaire) et l'on a* $M(1+in) = W\alpha$.

Au moment de l'initialisation, nous avons $M = 1$, $W = 1$ et $\alpha = 1+in$: les propriétés (T_1) et (T_3) sont donc vraies.
Reste (T_2). Tout d'abord, α ne possède pas de facteur irréductible du type (c). Sinon, on pourrait écrire $1+in = p(x+iy)$ (avec p premier de la forme $4k+3$) ce qui est absurde (regarder la partie réelle!). Si ξ irréductible divise α, sa norme $N(\xi)$ est donc un nombre premier qui divise $N(\alpha) = 1+n^2$. En vertu de (T), $N(\xi)$ divise un entier de la forme $1+d^2$, avec $0 < d < n$, ce qui termine (T_2).

$M := 1$; $\alpha := 1 + in$;
$W := 1$; (* *la variable* W *ne figure ici que pour faciliter la preuve* *)
tant que $N(\alpha) > 1$ **faire**
  rechercher un diviseur irréductible $u + iv$ *de* α;
  si $|u| = 1$ **faire**
    écrire $1 + iv/u$;
    $W := W(1 + iv/u)$;
    $\alpha := \alpha\, u/(u + iv)$
  sinon
    si $|v| = 1$ **faire**
      écrire $1 - iu/v$;
      $W := W(1 - iu/v)$;
      $\alpha := \alpha iv/(u + iv)$
    sinon
      rechercher $x + iy$ *tel que* $(x + iy)(u + iv) = 1 + iw$
      avec $|w|$ *minimum*;
      écrire $1 + iw$;
      si $|w| \geq n$ **alors**
        écrire "condition (T) non satisfaite";
        $\alpha := 1$ (* *fin de l'algorithme* *)
      sinon
        $M := M(x^2 + y^2)$;
        $W := W(1 + iw)$;
        $\alpha := \alpha(x - iy)/(u + iv)$
      fin si
    fin si
  fin si
fin tant que;
écrire α, M.

L'algorithme de TODD

Supposons maintenant qu'à un moment donné W, M, α vérifient (T_1), (T_2) et (T_3). Si α n'est pas une unité, l'algorithme recherche un diviseur irréductible $\xi = u + iv$ de α d'où $\alpha = (u + iv)\beta$. D'après (T_2), ξ est du type (a) ou (b).
Si l'on a $|u| = 1$ ou $|v| = 1$, W et α sont transformées en W' et α' et il est immédiat que W', M', α' vérifient (T_1), (T_2) et (T_3).
Si l'on a $|u| > 1$ ou $|v| > 1$, l'algorithme recherche $x + iy$ tel que $(x + iy)(u + iv) = 1 + iw$ avec $|w|$ minimum. L'hypothèse (T_2) nous apprend que $N(\xi) = p$ divise $1 + d^2$, avec $0 < d < n$. Le lemme 3 montre alors que $|w| \leq d < n$. Par conséquent W, M, α sont transformées en W', M' et

$$\alpha' = \alpha(x - iy)/(u + iv) = \beta(x - iy).$$

Les propriétés (T_1) et (T_3) sont encore vraies.
Terminons en montrant que $x - iy$ vérifie (T_2). Tout diviseur irréductible η de $x - iy$ divise aussi $1 + iw$. Les arguments employés au moment de l'initialisation sont encore valables et montrent que η est du type (a) ou (b). Enfin $N(\eta)$ divise $1 + w^2$ dont nous savons qu'il vérifie $|w| < n$.

Prouvons maintenant que l'algorithme s'arrête au bout d'un temps fini. Pour cela, il suffit de remarquer que l'on a $N(\alpha') < N(\alpha)/2$ si $|u| = 1$ ou $|v| = 1$. Sinon, on a $\alpha' = \beta(x - iy)$ d'où l'on déduit

$$N(\alpha') = N(\beta)\, N(x - iy) < N(\beta)\, N(u + iv)/3 < N(\alpha)/3$$

en appliquant la seconde partie du Lemme 3. Quel que soit le cas de figure, on a $N(\alpha') < N(\alpha)/2$. L'algorithme imprime donc r entiers de GAUSS, avec

$$r < \mathrm{E}\left[\log_2(1 + n^2)\right] + 1,$$

puis s'arrête en imprimant une unité.

Supposons maintenant que l'entier n ne vérifie pas la condition (T). Remplaçons la propriété (T_2) par la propriété (T_2') plus faible que voici :

(T_2') *α est un entier de* GAUSS. *Si ξ est un facteur irréductible de α, il est du type* (a) *ou* (b).

La preuve précédente s'adapte et montre qu'à chaque instant (T_1), (T_2') et (T_3) sont vraies.

Supposons alors que l'algorithme n'annonce pas "*la condition (T) n'est pas satisfaite*". Il fournirait dans ce cas — et en un temps fini — une formule *à la* MACHIN, ce qui est impossible.

Exemple : considérons l'entier $n = 19$.
Nous avons $1 + 19i = (1 + i)(10 + 9i)$. L'égalité $(x + iy)(10 + 9i) = 1$ exige $x = 1 + 9k$, $y = 1 + 10k$, $w = 19 + 181k$. La plus petite valeur de $|w|$ est donc 19 (obtenue pour $k = 0$). L'inégalité $|w| < 19$ n'est pas vérifiée : l'algorithme s'arrête signalant que 19 n'est pas décomposable.

5. Où il n'est plus question de fonction Arctangente.

Considérons l'égalité suivante, obtenue grâce à l'algorithme de TODD,

$$1850(1 + 266i) = -i(1 + i)(1 - 2i)^2(1 + 6i)(1 - 80i)(1 - 143i)$$

et qui, par passage aux arguments, nous fournit la formule *à la* MACHIN

$$\mathrm{Arctg}\,(266) = k\,\mathrm{Arctg}\,(1) - 2\,\mathrm{Arctg}\,(2) + \mathrm{Arctg}\,(6) - \mathrm{Arctg}\,(80) - \mathrm{Arctg}\,(143).$$

Il est frustrant, après des calculs d'arithmétique pure, d'avoir recours à une calculatrice pour déterminer la valeur exacte de

$$k = \Big[\mathrm{Arctg}\,(266) + 2\,\mathrm{Arctg}\,(2) - \mathrm{Arctg}\,(6) + \mathrm{Arctg}\,(80) + \mathrm{Arctg}\,(143)\Big] / \mathrm{Arctg}\,(1)$$

(la valeur de k est 7).

Nous allons voir comment on peut éviter cette fausse note.

Soit $W = a + ib$ un nombre complexe différent de 0. Choisissons pour l'argument θ de W la détermination

$$-\pi \leq \theta < 3\pi/2.$$

La raison de ce choix inhabituel est que l'on a

$$\theta = \mathrm{Arctg}\,(b/a) + c\pi$$

avec

$$c = \begin{cases} 0 & \text{si} \quad a \geq 0 \\ 1 & \text{si} \quad a < 0. \end{cases}$$

(Nous travaillons avec les conventions suivantes : $b/0 = \pm\infty$ selon le signe de b et $\mathrm{Arctg}\,(\pm\infty) = \pm\pi/2$.)

Soit $w \neq 0$ réel et posons $W' = W(1 + iw) = a' + ib'$. Si θ' est l'argument de W', nous savons que

$$\theta' = \theta + \mathrm{Arctg}\,(w) + 2k\pi.$$

Cherchons comment se calcule k en fonction des données. Pour cela, considérons $\mathrm{Arctg}\,(b'/a')$ et $\mathrm{Arctg}\,(b/a)$ comme fonctions de a. Ces fonctions, ayant la même dérivée, ne diffèrent que par une constante. Avec un peu de patience, on trouve que l'on a

$$\mathrm{Arctg}\,(b'/a') = \mathrm{Arctg}\,(b/a) + \mathrm{Arctg}\,(x) - d\pi$$

où d est un entier défini de la manière suivante

$$d = \begin{cases} 0 & \text{si} \quad a \notin]0, bw[\quad \text{et} \quad aa' \neq 0 \\ \mathrm{sgn}\, w & \text{si} \quad a \in]0, bw[\quad \text{et} \quad aa' \neq 0 \\ [\mathrm{sgn}\, w + \mathrm{sgn}\, b]/2 & \text{si} \quad a = 0 \\ [\mathrm{sgn}\, w - \mathrm{sgn}\, b]/2 & \text{si} \quad a' = 0. \end{cases}$$

(Vu les hypothèses, on ne peut pas voir simultanément $a = 0$ et $a' = 0$).
Ce travail effectué, en écrivant

$$\mathrm{Arctg}\,(b'/a') + c'\pi = \mathrm{Arctg}\,(b/a) + c\pi + \mathrm{Arctg}\,(w) + 2\pi,$$

on obtient

$$k = \begin{cases} 1 & \text{si} \quad a \geq 0 \quad \text{et} \quad a' < 0 \quad \text{et} \quad w < 0 \\ -1 & \text{si} \quad a < 0 \quad \text{et} \quad a' \geq 0 \quad \text{et} \quad w > 0 \\ 0 & \text{sinon.} \end{cases}$$

Reprenons notre exemple. A partir de $W = 1$, d'argument $\theta = 0$, on calcule successivement les arguments de

$(1+i)$,
$(1+i)(1-2i)$,
$(1+i)(1-2i)(1-2i)$,
.....
$(1+i)(1-2i)^2(1+6i)(1-80i)(1-143i)$,

ce qui donne la suite des arguments

$\text{Arctg}\,(1)$,
$\text{Arctg}\,(1) - \text{Arctg}\,(2)$,
$\text{Arctg}\,(1) - 2\,\text{Arctg}\,(2)$,
.....
$9\,\text{Arctg}\,(1) - 2\,\text{Arctg}\,(2) + \text{Arctg}\,(6) - \text{Arctg}\,(80) - \text{Arctg}\,(143)$.

Au lieu de regarder ce qui se passe quand on multiplie W par une unité ϵ, déterminons plutôt l'argument de $M(1+in)/\epsilon$. On trouve facilement

$$\text{Arctg}\,(M(1+in)/\epsilon) = \begin{cases} \text{Arctg}\,(n) & \text{si} \quad \epsilon = 1 \\ \text{Arctg}\,(n) + \text{Arctg}\,(1) & \text{si} \quad \epsilon = -1 \\ \text{Arctg}\,(n) - 2\,\text{Arctg}\,(1) & \text{si} \quad \epsilon = i \\ \text{Arctg}\,(n) + 2\,\text{Arctg}\,(1) & \text{si} \quad \epsilon = -i. \end{cases}$$

Dans notre exemple, cela donne

$$\text{Arctg}\left[1850(1+266i)/-i\right] = \text{Arctg}\,(266) + 2\,\text{Arctg}\,(1).$$

On obtient

$$\text{Arctg}\,(266) + 2\,\text{Arctg}\,(1) = 9\,\text{Arctg}\,(1) - 2\,\text{Arctg}\,(2) + \text{Arctg}\,(6) - \text{Arctg}\,(80) - \text{Arctg}\,(143)$$

ce qui donne la formule cherchée, soit

$$\text{Arctg}\,(266) = 7\,\text{Arctg}\,(1) - 2\,\text{Arctg}\,(2) + \text{Arctg}\,(6) - \text{Arctg}\,(80) - \text{Arctg}\,(143).$$

6. Quelques remarques avant de terminer.

Voici quelques conseils qui pourront être utiles à ceux qui seront tentés de programmer l'algorithme de TODD.

6.1. Comment décomposer un entier de GAUSS en facteurs irréductibles.

Soit $\alpha = \xi_1 \dots \xi_n$ une décomposition de α en facteurs irréductibles. D'après le théorème 2, $N(\alpha) = N(\xi_1) \dots N(\xi_n)$ est la décomposition de $N(\alpha)$ en facteurs premiers. Toujours d'après ce théorème, nous savons que

(a) si $N(\xi) = 2$ alors $\xi = 1 + i$,

(b) si $N(\xi) = p$, avec p premier de la forme $4k+1$, alors $\xi = a+ib$ ou $\xi = b+ia$, a et b étant deux entiers > 0 tels que $p = a^2 + b^2$,

(c) si $N(\xi) = p^2$, avec p premier de la forme $4k + 3$, alors $\xi = p$.

La construction d'un algorithme pour décomposer α en facteurs irréductibles va maintenant de soi, sauf dans le cas (b). Comment en effet, trouve-t-on les entiers a et b? Plutôt que de décrire une méthode sophistiquée (**)
pour obtenir ce résultat, je me contenterai d'indiquer comment on peut utiliser la force brute avec discernement.

De $p = a^2 + b^2$ avec $0 < a < b$, on déduit $a < \sqrt{p/2} < b < \sqrt{p}$. Les intervalles dans lesquels se trouvent a et b ont pour longueurs $\sqrt{p/2} = 0,707\sqrt{p}$ et $\sqrt{p} - \sqrt{p/2} = 0,292\sqrt{p}$. D'où l'algorithme

---

$b := 1 + E\left(\sqrt{p/2}\right)$; (* E *désigne la partie entière* *)
$a := E\left(\sqrt{p - b^2}\right)$;
tant que $p \neq a^2 + b^2$ **faire**
$b := b + 1$;
$a := E\left(\sqrt{p - b^2}\right)$
fin tant que.

L'expérience prouve que cette procédure n'est pas trop catastrophique tant que l'on manipule de petites valeurs de p (si p possède au plus neuf chiffres on a $0,292\sqrt{p} < 29\,290$).

6.2. Comment trouver une solution particulière de $ax + by = 1$.

Soient a et b deux entiers premiers entre eux. Pour trouver facilement une solution particulière de l'équation, en nombres entiers, $ax+by = 1$, voici un algorithme qui a été décrit en 1963 par BLANKINSHIP. L'idée est d'utiliser la méthode du pivot de GAUSS, en l'adaptant aux entiers. Je me contenterai d'un exemple, avec $a = 35$ et $b = 22$.
On part de la matrice 2×3

(**) Le lecteur intéressé par ce problème pourra lire avec profit un article très intéressant de Roger CUCULIÈRE dans le N° 102 d'Avril 1986 de "POUR LA SCIENCE", article consacré à ce théorème.

$$\begin{pmatrix} 35 & 1 & 0 \\ 22 & 0 & 1 \end{pmatrix}$$

On choisit 22 comme pivot, et on enlève à la première ligne de cette matrice E(35/22)=1 fois la deuxième ligne, ce qui donne la matrice

$$\begin{pmatrix} 13 & 1 & -1 \\ 22 & 0 & 1 \end{pmatrix}$$

On choisit 13 comme pivot et on enlève à la deuxième ligne E(22/13)=1 fois la première ligne, ce qui donne la matrice

$$\begin{pmatrix} 13 & 1 & -1 \\ 9 & -1 & 2 \end{pmatrix}$$

On continue ainsi à jouer au ping-pong jusqu'à ce que l'un des éléments de la première colonne soit nul. Les matrices obtenues sont

$$\begin{pmatrix} 4 & 2 & -3 \\ 9 & -1 & 2 \end{pmatrix} \quad \begin{pmatrix} 4 & 2 & -3 \\ 1 & -5 & 8 \end{pmatrix} \quad \begin{pmatrix} 0 & 22 & -35 \\ 1 & -5 & 8 \end{pmatrix}$$

Dans la deuxième ligne de la dernière matrice obtenue, on trouve le pgcd $1 = (35, 22)$ puis $x = -5$ et enfin $y = 8$. Vérification : $-5 \times 35 + 8 \times 22 = 1$.

6.3. Liste des 30 premières formules à la MACHIN.

(pour simplifier les notations, nous avons remplacé Arctg (n) par (n) seulement)

$$\begin{aligned}
(3) &= 3(1) - (2) \\
(7) &= -(1) + 2(2) \\
(8) &= 5(1) - (2) - (5) \\
(13) &= 5(1) - (2) - (4) \\
(17) &= (1) + 2(2) - (12)
\end{aligned}$$

$$\begin{aligned}
(18) &= 3(1) - 2(2) + (5) \\
(21) &= 2(1) + (4) - (5) \\
(30) &= 7(1) - (2) - (4) - (23) \\
(31) &= 2(1) + (5) - (6) \\
(32) &= (1) + 2(2) - (9)
\end{aligned}$$

$$\begin{aligned}
(38) &= -(2) + 2(4) \\
(41) &= (1) - 2(2) + 2(12) \\
(43) &= 3(1) - 2(2) + (6) \\
(46) &= 3(1) + 2(2) - (12) - (27) \\
(47) &= 4(1) + (2) - (4) - (5)
\end{aligned}$$

$$\begin{aligned}
(50) &= 2(1) + (9) - (11) \\
(55) &= 4(1) + (4) - (5) - (34) \\
(57) &= -4(1) + 3(2) + (5) \\
(68) &= 8(1) - 3(2) - (6) \\
(70) &= -2(1) - (2) + 2(5) + (12)
\end{aligned}$$

$$\begin{aligned}
(72) &= -3(1) + (2) + (4) + (11) \\
(73) &= 7(1) - (2) - (5) - (9) \\
(75) &= 3(1) + 2(2) - (12) - (22) \\
(76) &= 2(1) + (23) - (33) \\
(83) &= 5(1) - 2(2) + (5) - (23)
\end{aligned}$$

$$\begin{aligned}
(91) &= 2(1) + (9) - (10) \\
(93) &= 5(1) - 2(2) + (6) - (80) \\
(98) &= 7(1) - (2) - (4) - (15) \\
(99) &= 5(1) - (2) - 2(5) + (12) \\
(100) &= 2(1) + (27) - (37).
\end{aligned}$$

6.4. Quelques questions naturelles.

La formule (M) peut se généraliser dans deux directions.

Tout d'abord, on peut se demander ce qui se passe lorsque n est un nombre *rationnel.* Par exemple, on a l'égalité

$$\text{Arctg}\,(100/17) = \text{Arctg}\,(6) + \text{Arctg}\,(290) - \text{Arctg}\,(4836),$$

et on peut démontrer que toute fraction a/b fournit une formule *à la* MACHIN. On se reportera à l'article de TODD pour y trouver un algorithme très simple.

On peut aussi prendre pour les c_i des nombre rationnels. La formule de GAUSS, citée au début, est un exemple. Cette formule peut cependant s'obtenir comme combinaison linéaire de formules *à la* MACHIN (essayez!). Dans son article, TODD affirme que l'on n'obtient rien de nouveau, mais il ne donne pas de justification. Un lecteur perspicace saura-t-il répondre?

Il en a enfin une dernière question inévitable. Un entier décomposable n peut donner naissance à plusieurs formules *à la* MACHIN. Telle quelle, cette question est mal posée. Nous avons en effet obtenu les formules

$$\begin{aligned}\text{Arctg}\,(342) &= -\text{Arctg}\,(1) + 2\,\text{Arctg}\,(2) - \text{Arctg}\,(5) + \text{Arctg}\,(44) - \text{Arctg}\,(129)\\ &= -3\,\text{Arctg}\,(1) + 2\,\text{Arctg}\,(2) - \text{Arctg}\,(5) + \text{Arctg}\,(28) + \text{Arctg}\,(44)\end{aligned}$$

parce que 129 est décomposable. Soyons plus précis : peut-on obtenir deux formules (M) ne faisant intervenir que des entiers i indécomposables? Autrement dit, la famille des entiers indécomposables est-elle libre sur $\mathbf{Q}$? Je ne sais pas répondre à cette question. Là encore, les lecteurs de "*L'OUVERT*" sont sollicités...

Bibliographie

John TODD : *A problem on Arctangent Relations* — American Math. Monthly 56(1949) 517 - 528.

(Cet article contient beaucoup d'autres résultats dont je n'ai pas le temps de parler ici.)

W.-A. BLANKINSHIP : *A New Version of the Euclidean Algorithm* — American Math. Monthly 70(1963) 742 - 745.