数理解析研究所講究録
第581巻 1986年 1-6

根号による1のn乗根の解法

電子技術総合研究所　元吉文男　(Fumio Motoyoshi)

1．はじめに

1のn乗根は任意の正数nに対して根号によって表わされることが知られているが、これを実際に計算機で求めるプログラムを作成したので報告する。この際、従来から知られていた方法に手を加え、計算量を考慮したアルゴリズムになるようにした。また根号の扱いについても計算機で機械的に処理するのに適した解釈をするようにした。ここでは、まずこの根号の解釈法を述べ、次に1のn乗根を求める実際のアルゴリズムを解説する。最後にこのアルゴリズムによって求められた1の7乗根と13乗根をしめしておく。

2．根号の解釈

xのn乗根 $a=\sqrt[n]{x}$ というのはn乗してxになる数のことであるが、このような数はn個あり、aによってそのうちのどれを表わすかが問題となる。xが正の実数のときは普通はaは正の実数になるようにしている。しかしxが複素数のときにはどれにするかが明らかではない。主値をとるという偏角を最小にする方法もあるが、これでも問題が生じることがある。たとえば3次方程式（1）が与えられたときに、t_1 と t_2 を（2）で示さ

$$x^3+px+q=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (1)$$

$$t_1=-\frac{q}{2}+\sqrt{\left(\frac{p}{2}\right)^2+\left(\frac{q}{3}\right)^3}\ , \quad t_2=-\frac{q}{2}-\sqrt{\left(\frac{p}{2}\right)^2+\left(\frac{q}{3}\right)^3} \quad (2)$$

$$x=\sqrt[3]{t_1}+\sqrt[3]{t_2} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (3)$$

れる値としたときに、（３）で示されるｘが根であるとするが、このときにはt_1の３乗根とt_2の３乗根のとりかたは独立ではなく、その積が$-p/3$であるという関係がある。そこでいつも主値をとるようにしていたのでは不都合が生じる。

ここでは根号を次のように解釈することにする。すなわち、根号で示される式は、そのどの分岐をとってもよいようにする。ただしいったん分岐を定めたならば、次からは同じ式が根号の中に入る場合には前と同じ分岐をとることにする。この条件はもうすこし緩めることが可能で、実際、同じところで根号をとったものだけを同じ分岐にするようにしても以後の計算に不都合は生じない。しかし、これでは出力のときにどの根号どうしが同じ分岐であるかをいちいち指定しなくてはならず不便であるので最初に述べた方策に従うことにした。ただし、こうすることによって上の例における（３）式のような書き方が許されなくなる。すなわち、（３）における２つの根号は分岐のとりかたが相互に依存しているからである。ここでの根号の解釈の仕方によると、（３）の根は次のように表わすことになる。

$$x=\sqrt[3]{t_1}-\frac{p}{3\sqrt[3]{t_1}} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (4)$$

すなわち、分岐のとりかたが依存しているような根号は一つの根号で表わさなければならない。（４）式では分岐のとりかたによって自動的に３つの根が表現されている。

３．“１”の原始ｎ乗根の解法

１の原始ｎ乗根をω_nとする。原始ｎ乗根というのは次の式を満たす数のことである。

$$\omega_n^n=1 \quad \text{かつ} \quad \omega_n^m\neq 1 \quad 0<m<n.$$

まずｎが素数の場合に帰着されることを示す。

Ⅰ．$n=p^k$のとき（ｐは素数）

$\omega_n=\sqrt[k]{\omega_p}$が１の原始ｎ乗根となる（どの分岐をとっても）。

II．n＝pqのとき（pとqは互いに素）

$x=\omega_p\omega_q$を考える。このとき、$\omega_p=\omega_{pq}^{q}=\omega_n^{q}$、$\omega_q=\omega_{pq}^{p}=\omega_n^{p}$と書ける。

すると$x=\omega_n^{p+q}$となるが、gcd(n，p＋q)＝1なので

xが1の原始n乗根である。

nが素数でない場合は上の2つで尽くされており、これらを繰り返し適用することによって、nが素数の場合に帰着される。nが素数の場合の解法を以下に示すが、そこでは、前節で述べた根号の解釈にあてはまるようになっており、分岐のとりかたが相互に依存する根号が存在しないようになっている。

ω_nを1の原始n乗根とすると、nが素数の場合はRを有理数としたときにG(R(ω_n)，R)がn－1次の巡回群になる。ここでG(A，B)は体Bの上の体Aのガロア群である。このとき、G_0＝G(R(ω_n)，R)とすると次のような可解列G_iが存在する：

$G_0\supset G_1\supset\cdots\supset G_m=e$，

ただしG_{j-1}/G_jは素数次の巡回群（$0<i\leqq m$）．

各G_jに対応する体をそれぞれR_jとしてG_{j-1}/G_jの次数をp_jとおくと、$R_{j-1}=R_j(\eta_j)$となっている。ここでη_jはG_j上のある既約p_j次方程式の根である。この方程式を求め、それをラグランジェの分解式を使用して解けばよい。以下に述べる方法では、方程式を求める部分とそれを解く部分をまとめてある。そのため、方程式は直接には表われて来ない。

III．nが素数のとき

次のような整数列f_jを求める：

$n-1=f_0>f_1>\cdots>f_m=1$，

ただし、各f_jはf_{j-1}を割り切り、$p_j=f_{j-1}/f_j$は素数であり、

かつ$p_{j-1}\geqq p_j$とする（$1\leqq j\leqq m$について）。

$e_j=(n-1)/f_j$としておく。

2）nの原始根をrとし、$\zeta_0=\omega_n$，$\zeta_{i+1}=\zeta_i^{r}$とする

（$0\leqq i<n-1$）

ここでの計算はω_nを変数とみなして、ω_nに関する多項式として計算を進める。

なおこの計算の際に ω_n の n 次以上の項は次の関係により消去することができる。

$$\omega_n^n - 1 = 0$$

以後の計算においても同様に行う。

3) $\eta_{0,0} = \zeta_0 + \zeta_1 + \cdots + \zeta_{n-2}$
$= \omega_n + \omega_n^2 + \cdots + \omega_n^{n-1}$
$= -1$

とし、次のことを各 j について行う（$1 \leqq j \leqq m$）。

3．1) 1) における e_j, e_{j-1}, f_j を使用して

$$\eta_{j,i} = \zeta_{ie_{j-1}} + \zeta_{e_j+ie_{j-1}} + \cdots + \zeta_{(f_j-1)e_j+ie_{j-1}}$$
$(0 \leqq i < p_j)$

を計算する（ガウスの f_j 項周期）

3．2) $\eta_{j,0}$ を次の手順に従って求める。

i) III の手続きを再帰的に使用して 1 の原始 p_j 乗根 ω_{p_j} を求める。

ii) ラグランジュの分解式を次のように求める。

$$<\omega_{p_j}^k, \eta_j> = \sum_{i=0}^{p_j-1} \omega_{p_j}^{ik} \eta_{j,i}$$ と定義する。・・・・・・・・（＊）

このとき $<\omega_{p_j}^0, \eta_j> = \sum_{i=0}^{p_j-1} \eta_{j,i} = \eta_{j-1,0}$ である。

また $u_{j,k} = <\omega_{p_j}^k, \eta_j><\omega_{p_j}, \eta_j>^{p_j-k}$ は ω_n の多項式であるが、

これは $\eta_{j-1,0}$ を表わす ω_n の式を使用して ω_n を消去できることが知られている（$1 \leqq k < p_j$）

$\eta_{j-1,0}$ はすでに根号で表わされているので $\eta_{j,k}$ も根号で表わせる。

この $u_{j,k}$ を使用して

$$<\omega_{p_j}, \eta_j> = \sqrt[p_j]{u_{j,1}}$$

がまず求まり、

$2 \leqq k < p_j$ については

$$<\omega_{p_j}^k, \eta_j> = u_{j,k} <\omega_{p_j}, \eta_j>^{p_j-1} = u_{j,k} <\omega_{p_j}, \eta_j>^k / u_{j,1}$$

によって求まる。

ここで（＊）の式について０からp_j-1まで加えると、

$$p_j \eta_{j,0} = \sum_{k=0}^{p_j-1} <\omega_{p_j}^{k}, \eta_j>$$

となり、$\eta_{j,0}$が根号によって表わされる。

4）　3）によって求めた$\eta_{j,0}$が１の原始ｎ乗根　　である。

注）

3）における繰り返しにおいて最後のｊ＝ｍの場合は実は次のように簡単に計算できる。

ｎは２と異なる素数と考えてよいので、ｎ－１は偶数となり

$f_{m-1}=2$となる。このとき$r^{n-1}=1$（ｍｏｄ　ｎ）から

$r^{(n-1)/2}=-1$（ｍｏｄ　ｎ）がいえるので

$$\eta_{m-1,0}=\xi_0+\xi_{(n-1)/2}=\omega_n+\omega_n^{r^{(n-1)/2}}=\omega_n+\omega_n^{-1}$$

となり これを変形して

$$\omega_n^2-\eta_{m-1,0}\omega_n+1=0$$

となるので、直ちに解くことができて、次の式が得られる：

$$\omega_n=(\eta_{m-1,0}+\sqrt{\eta_{m-1,0}^2-4})/2。$$

４．例

３で述べたアルゴリズムを使用して実際に１の７乗根と１３乗根を計算した例を次ページに示す。そこで使用されている記号について説明する。

Ｗ（ｎ）はω_nを示す。１つの式にすると長すぎるので根号の中が数字でない場合には、＠２などと書いて後でその値を示している。根号は｜で表わし

｜ｘは$\sqrt{x}$を、ｎ｜ｘは$\sqrt[n]{x}$を表わすものとする。またｘ＾ｎはx^nを表わす。

W(7)=(4 !@2 + 3 !3 i 3!@1^2 + 3!@1^2 + 28 3!@1 - 56)/336

@1=28 (- 3 !3 i + 1)

@2=21 (- !3 i 3!@1^2 + 2 3!@1^2 + 7 !3 i 3!@1 - 7 3!@1 - 196)

W(13)=(2 !@5 + 4 !@4 + 3 !3 i 3!@3^2 - 5 3!@3^2 + 52 3!@3 - 104)/1248

@3=52 (- 3 !3 i - 5)

@4=39 (- 3 !3 i 3!@3^2 - 8 3!@3^2 - 39 !3 i 3!@3 + 13 3!@3 + 676)

@5=2 (3 !3 i 3!@3^2 !@4 - 5 3!@3^2 !@4 + 52 3!@3 !@4 - 104 !@4 - 312 !3 i 3!@3^2 - 156 3!@3^2 - 2028 !3 i 3!@3 - 2028 3!@3 - 105456)

記号の意味：

x ^ n は x^n，

! x は$\sqrt{x}$，n ! x は$\sqrt[n]{x}$ を表わす