Astérisque

R. F. CHURCHHOUSE

Efficient computation of algebraic continued fractions

Astérisque, tome 38-39 (1976), p. 23-32

<http://www.numdam.org/item?id=AST_1976__38-39__23_0>

Société Mathématique de France
Astérisque 38-39 (1976) p.23-32

EFFICIENT COMPUTATION OF ALGEBRAIC CONTINUED FRACTIONS

by

R.F. CHURCHHOUSE

1.- INTRODUCTION

From time to time problems arise in the Theory of Numbers which call for extensive multilength computations as part of their solution. The number of such problems is likely to increase in the future partly at least as a result of the relatively recent discoveries by Alan Baker, of which [1] might be regarded as typical, which enable us to make statements of the type that if a certain Diophantine Equation has any solutions at all then these solutions are bounded by a specific, computable, constant. The search for solutions can then be restricted to a finite, though possibly very large, region in the appropriate space. Before we can attack such problems on a computer we therefore need a good general - purpose multi-length arithmetic package.

Some years before I left the Atlas Laboratory we were able to acquire a very fine multi-length package written by W.F. Lunnon and during the period 1967 - 1971 we carried out some extensive computations of algebraic continued fractions to a precision equivalent to several hundred places of decimals. In the course of this work we were able to assist Baker and Davenport [2] in their proof that there are no solutions of a certain set of Diophantine Equations and Muir and I [3] were able to solve a problem in-

volving the remarkable continued fraction associated with the positive root of the cubic $x^3 - 8x - 10 = 0$.

Multi-length computation of continued fractions was also necessary in the successful factorisation of F_7, the seventh Fermat number, by Morrison and Brillhart [4] using a method proposed by D.H. Lehmer many years before. The essential idea in Lehmer's method is to find the continued fraction expansion of $\sqrt{kN}$ where N is the number to be factorised and k is given various integer values. The convergents so found give rise to a set of quadratic congruences (mod N) and if a subset of these can be found which have the property that the product of their residues is a perfect square we may be able to find a factor of N (but the factor may turn out to be 1 !).

2.- SOME PROPERTIES OF CONTINUED FRACTIONS

For the sake of completness the essential properties of continued fractions are summarised below.

i) If $\underline{\theta}$ is any positive real number let :

$$a_o = [\underline{\theta}] \quad \text{and} \quad r_o = (\underline{\theta} - a_o)^{-1}$$

where, as usual, $[x]$ denotes the integral part of x.

Define also, for $n \geqslant 0$:

$$a_{n+1} = [r_n] \ , \ r_{n+1} = (r_n - a_{n+1})^{-1} \ .$$

Then we say that $\underline{\theta}$ has the continued fraction representation :

$$\underline{\theta} = a_o + \frac{1}{a_1 +} \frac{1}{a_2 +} \frac{1}{a_3 + \cdots} \qquad (1)$$

The elements a_o, a_1, a_2, ... are called "the partial quotients". If we truncate the expansion (1) after 1,2,3,... terms we obtain a series of rational approximations to $\underline{\theta}$:

$$\frac{p_o}{q_o} = \frac{a_o}{1} \ , \ \frac{p_1}{q_1} = \frac{a_o a_1 + 1}{a_1} \ , \ \frac{p_2}{q_2} = \frac{a_o a_1 a_2 + a_2 + a_o}{a_1 a_2 + 1} \quad \text{etc}$$

where, more generally :

$$\left.\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2} \\ \text{and} \qquad q_n &= a_n q_{n-1} + q_{n-2} \end{aligned}\right\} \quad (n \geqslant 2)$$

The fractions p_n/q_n so obtained are called "the convergents to $\underline{\theta}$ "; they are always in their lowest terms and provide the best possible approximations to $\underline{\theta}$ in the sense that :

$$|\underline{\theta} - \frac{p_n}{q_n}| < |\underline{\theta} - \frac{P}{Q}| \quad \text{for all } Q < q_n.$$

Furthermore, for all n :

$$|\underline{\theta} - \frac{p_n}{q_n}| < \frac{1}{q_n^2} .$$

ii) The continued fraction for $\underline{\theta}$ terminates if, and only if, $\underline{\theta}$ is rational.

iii) The continued fraction for $\underline{\theta}$ is periodic if, and only if, $\underline{\theta}$ is a quadratic irrational.

An unsolved problem of major importance is whether or not the partial quotients of the continued fraction of algebraic numbers of the third or higher degrees are bounded. If this question could be answered a good deal of progress might be made in several branches of the Theory of Numbers.

Having briefly summarised some of the reasons why extensive computation of the continued fractions of algebraic numbers of the third and higher degrees is important I now turn to the main topic of this paper: how can such continued fractions be computed most efficiently ? In the next two sections I shall describe the two commonly used methods of computation, to which I give the names : (i) the Direct method, and (ii) the Chain method. In section 5 I shall then compare the efficiencies of the two methods.

3.- THE DIRECT METHOD

Let $\underline{\theta}$ be a real algebraic number of degree k satisfying the irreducible polynomial :

$$f(x) \equiv c_k x^k + c_{k-1} x^{k-1} + \ldots + c_1 x + c_o = 0 \qquad (2)$$

where the c_i are integers. We can find the value of $\underline{\theta}$ on a computer, to within an accuracy determined by the word-length, by the use of the Newton-Raphson or some other appropriate method. Suppose that the approximate value of $\underline{\theta}$ so obtained is $\underline{\theta}'$ and that $\underline{\theta}'$ is accurate to n places of decimals, then :

$$|\underline{\theta} - \underline{\theta}'| < \frac{1}{2} \times 10^{-n} .$$

We now expand $\underline{\theta}'$ as a continued fraction according to the algorithm defined in the previous section and so obtain the first m partial quotients:

$$\underline{\theta}' \doteq a_o + \frac{1}{a_1 +} \frac{1}{a_2 + \ldots} \frac{1}{a_{m-1}} .$$

The crucial question is : how many of these m numbers are in fact partial quotients of $\underline{\theta}$ itself ?

We cannot give a theoretical answer to this question which is sufficiently precise to be of use in dealing with any specific number, $\underline{\theta}$, so we adopt what might be called an experimental approach : we compute the continued fractions of two numbers close to $\underline{\theta}'$ such as :

$$\underline{\theta}'_+ = \underline{\theta}' + \underline{\epsilon}$$

$$\underline{\theta}'_- = \underline{\theta}' - \underline{\epsilon}$$

where $\underline{\epsilon}$ is a small number $\geqslant \frac{1}{2} \times 10^{-n}$. It follows that $\underline{\theta}$ certainly satisfies :

$$\underline{\theta}'_- < \underline{\theta} < \underline{\theta}'_+ .$$

By comparing the partial quotients of $\underline{\theta}'$, $\underline{\theta}'_+$ and $\underline{\theta}'_-$ and accepting only those which are identical in all three expansions we may be sure that all those accepted are certainly partial quotients of $\underline{\theta}$.

As an example of this approach we compute the first few partial quotients of $2^{1/3}$.

To 7 signifiant figures the value is 1.259921. For simplicity we take $\underline{\epsilon} = 10^{-6}$ and therefore compute the continued fractions for :

$$\underline{\theta}'_{-} = 1.259920 = 1 + \frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{5+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{4+}\,\frac{1}{2+}\ \ldots$$

$$\underline{\theta}' = 1.259921 = 1 + \frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{5+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{4+}\,\frac{1}{1+}\ \ldots$$

$$\underline{\theta}'_{+} = 1.259922 = 1 + \frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{5+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{4+}\,\frac{1}{1+}\ \ldots$$

We accept only the first 7 terms as correct and so write :

$$2^{1/3} = 1 + \frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{5+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{4+}\ \ldots$$

We now return to the question asked above and see if we can find an estimate for the number of partial quotients of $\underline{\theta}$ which will be correct when we use the Direct method when we work to an accuracy of n decimal places. Under these conditions we have :

$$|\underline{\theta} - \underline{\theta}'| \leqslant \frac{1}{2} \times 10^{-n} .$$

On the other hand we have no reason to believe that $|\underline{\theta} - \underline{\theta}'|$ will be much smaller than $\frac{1}{2} \times 10^{-n}$ and, since we wish to be sure that any partial quotients we accept really are correct we must assume that :

$$|\underline{\theta} - \underline{\theta}'| \doteqdot \frac{1}{2} \times 10^{-n} . \qquad (3)$$

We compute the continued fraction for $\underline{\theta}'$ and form the convergents :

$$\frac{p_o}{q_o} , \frac{p_1}{q_1} , \ldots , \frac{p_s}{q_s} .$$

Now, from the theory of continued fractions :

$$|\theta - \frac{p_r}{q_r}| < \frac{1}{q_r^2} \qquad (4)$$

and so, comparing (3) and (4), we see that we can have no confidence in the validity of p_r/q_r as a convergent to $\underline{\theta}$ if :

$$q_r^2 > 2 \times 10^n. \qquad (5)$$

Note that this result is independent of k, the degree of the polynomial satisfied by $\underline{\theta}$.

4.- THE CHAIN METHOD

We again suppose that $\underline{\theta}$ is a real algebraic number of degree k satisfying the irreducible polynomial (2) given above. By any convenient method we find the integer part of $\underline{\theta}$ and we write

$$\underline{\theta} = a_o + \frac{1}{\underline{\theta}_1}$$

where $\underline{\theta}_1 > 1$; we substitute this expression for $\underline{\theta}$ in (2) and so obtain an equation of the k-th degree satisfied by $\underline{\theta}_1$:

$$f_1(x) \equiv c_k^{(1)} x^k + c_{k-1}^{(1)} x^{k-1} + \ldots + c_o^{(1)} = 0 . \qquad (6)$$

The $c_i^{(1)}$ are integers and it is easy to see that, in fact :

$$c_{k-m}^{(1)} = \frac{f^{(m)}(a_o)}{m!}$$

where $f^{(m)}$ denotes the m-th derivative.

Similarly we find the integer part of $\underline{\theta}_1$ so that :

$$\underline{\theta}_1 = a_1 + \frac{1}{\underline{\theta}_2}$$

where $\underline{\theta}_2 > 1$ and by substituting for $\underline{\theta}_1$ in (6) we obtain the k-th degree equation satisfied by $\underline{\theta}_2$:

$$f_2(x) \equiv c_k^{(2)} x^k + c_{k-1}^{(2)} x^{k-1} + \ldots + c_o^{(2)} = 0 \qquad (7)$$

and so on.

This process can be continued so long as we can accurately represent in the computer all of the integers which occur as coefficients in the chain

of polynomials $f(x)$, $f_1(x)$, $f_2(x)$,... As an example consider again the continued fraction for $2^{1/3}$. We begin with its defining cubic :

$$x^3 - 2 = 0 \ , \quad \text{then } a_o = 1$$

and so the second cubic in the chain is :

$$x^3 - 3x^2 - 3x - 1 = 0, \quad \text{so that } a_1 = 3$$

and the third cubic in the chain is :

$$10x^3 - 6x^2 - 6x - 1 = 0 \ , \quad a_2 = 1$$

and so on. If we suppose that our computer can accurately represent all integers of absolute value $< 10^6$ we find that we obtain 13 terms of the continued fraction before the method fails because of overflow. The terms are :

$$2^{1/3} = 1 + \frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{5+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{4+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{8+}\,\frac{1}{1+}\,\frac{1}{14+}\,\frac{1}{1+}\ \ldots$$

a considerable improvement on the 7 terms obtained by the Direct method on a machine of comparable precision.

In using the Chain method we have not had to make any approximations so that every partial quotient obtained is certainly a partial quotient of $\underline{\theta}$ itself. We therefore need only estimate the number of polynomials in the chain we can compute before we must expect one of the coefficients to be too large to be represented accurately in the computer.

After m partial quotients have been obtained by the Chain method we will have formed the k-th degree polynomial for the number $\underline{\theta}_m$ where :

$$\underline{\theta} = a_o + \frac{1}{a_1+}\,\frac{1}{a_2+}\ \ldots\ \frac{1}{a_{m-1}+}\,\frac{1}{\underline{\theta}_m} \ .$$

If p_o/q_o , p_1/q_1 , ..., p_{m-1}/q_{m-1} are the corresponding convergents the relationship beween $\underline{\theta}$ and $\underline{\theta}_m$ can be expressed as :

$$\underline{\theta} = \frac{p_{m-1}\,\underline{\theta}_m + p_{m-2}}{q_{m-1}\,\underline{\theta}_m + q_{m-2}} \qquad (8)$$

and if we now substitute this expression for $\underline{\theta}$ into the polynomial (2) which defines it we obtain the polynomial for $\underline{\theta}_m$ in the form :

$$f_m(x) \equiv \sum_{r=0}^{k} a_r (p_{m-1}x + p_{m-2})^r (q_{m-1}x + q_{m-2})^{k-r} = 0 \qquad (9)$$

The leading coefficient of this polynomial is :

$$\sum_{r=0}^{k} a_r \, p_{m-1}^r \, q_{m-1}^{k-r}$$

or :

$$q_{m-1}^k \left(\sum_{r=0}^{k} a_r \left(\frac{p_{m-1}}{q_{m-1}}\right)^r \right) \qquad (10)$$

Now

$$\sum_{r=0}^{k} a_r x^r = a_k (x - \theta) \prod_{r=1}^{k-1} (x - \theta^{(r)})$$

where $\theta^{(r)}$ $(r = 1,2,\ldots,k-1)$ are the algebraic conjugates of θ hence

$$\sum_{r=0}^{k} a_r \left(\frac{p_{m-1}}{q_{m-1}}\right)^r = a_k \left(\frac{p_{m-1}}{q_{m-1}} - \theta\right) \prod_{r=1}^{k-1} \left(\frac{p_{m-1}}{q_{m-1}} - \theta^{(r)}\right) . \qquad (11)$$

As $q_{m-1} \to \infty$ the factor in the product in (11) approaches the constant value :

$$\prod_{r=1}^{k-1} (\theta - \theta^{(r)}).$$

On the other hand, from the theory of continued fractions, the factor :

$$\frac{p_{m-1}}{q_{m-1}} - \theta$$

approaches zero at a speed proportional to q_{m-1}^{-2} and it therefore follows that :

$$q_{m-1}^k \left(\sum_{r=0}^{k} a_r \left(\frac{p_{m-1}}{q_{m-1}}\right)^r \right) = O(q_{m-1}^{k-2}) \qquad (12)$$

as $q_{m-1} \to \infty$.

Analysis of the other coefficients of the polynomial (9)is more difficult, except for the constant term which can be proved to be $O(q_{m-2}^{k-2})$ but there is no reason to believe that any of the coefficients will be very different in absolute value from the estimate given by (12). On this assumption, which has been borne out by extensive calculations, it follows that the chain of polynomials will continue to be correctly computed on a machine

of n decimal digits integer precision for m steps where :

$$q_{m-1}^{k-2} \doteq 10^{n}. \qquad (13)$$

5. COMPARAISON OF THE EFFECTIVENESS OF THE TWO METHODS

We now have all the information necessary to prove :

THEOREM.- Let $D(n,k)$ and $C(n,k)$ the number of partial quotients of the continued fraction of an algebraic number of degree k that are computable on a machine of precision n decimal places by the Direct and Chain methods respectively. Then as $n \to \infty$:

$$C(n,2)/D(n,2) \to \infty$$

$$C(n,3)/D(n,3) > 1$$

$$C(n,4)/D(n,4) \doteq 1$$

$$C(n,k)/D(n,k) \to 0 \quad \text{for } k \geqslant 5.$$

Proof.- From (12)

$$C(n,k) = r \text{ where } q_r = O(10^{n/(k-2)})$$

From (5)

$$D(n,k) = s \text{ where } q_s = O(10^{n/2})$$

and the theorem follows at once when $k = 2,3,4$ and when $k \geqslant 5$ by comparison of the exponents.

Q.E.D

The case $k = 3$ is particulary interesting. We see that $C(n,3) = r$ where $q_r = O(10^n)$ and $D(n,3) = s$ where $q_s = O(10^{n/2})$. It is tempting to conjecture that $q_{2r} = O(q_r^2)$ and this is true if the partial quotients of a cubic irrational do not possess some remarkable properties. It seems unlikely that cubic irrationals do in general possess such properties and so we put forwards the

Conjecture.- $C(n,3)/D(n,3) \to 2$ as $n \to \infty$.

REFERENCES

[1] BAKER A. :"Linear forms in the logarithms of algebraic numbers" Mathematika, 15 (1968), 204-216.

[2] BAKER A. and DAVENPORT H. : "The equation $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$" Quart. Journal Maths. 20 (1969), 129-137.

[3] CHURCHHOUSE R.F and MUIR ; STE : "Continued fractions,algebraic numbers and modular invariants" Journ. Inst. Maths. and its Applications 5 (1969) 318-328.

[4] MORRISSON M.A and BRILLHART J. : "A method of factoring and the factorisation of F_7" Maths. Comp. 29 (1975) 183-205.

R.F. CHURCHHOUSE
Department of Computing Mathematics
University College
Mathematics Institute
Senghennydd Road
CARDIFF (Wales)
Grande-Bretagne