

## 平方根の任意多倍長計算法の例

堀田 涼	田中 輝雄	牧野 潔夫
工学院大学	工学院大学	工学院大学
Ryo Horita	Teruo Tanaka	Isao Makino
Kogakuin University	Kogakuin University	Kogakuin University

### 1 はじめに

われわれは整数の三則をできるだけ多く使い、浮動小数点演算の計算をできるだけ避けて任意精度の関数の値を求める研究を行っている。これまでに連分数を用いた手法により  $\log(1+z)$ ,  $\exp(z)$ ,  $\tan(z)$ ,  $\arctan(z)$  の任意精度計算を Risa/Asir に実装した<sup>[1]</sup>。

本論文では Risa/Asir の機能拡張を目的とし、連分数、漸化式、ニュートン法の 3 つの手法を用いた平方根の任意精度計算を行った。いずれの方法も整数の三則（加算、減算、乗算）を主とし、除算は 1 回のみで実装する。また、べき乗計算は binary 法を用いる。

### 2 連分数を用いた近似値の求め方

#### 2.1 連分数について

##### 2.1.1 連分数

分母に分数が含まれるような分数を連分数と呼ぶ。

$$q_0 + \frac{p_1}{q_1 + \frac{p_2}{q_2 + \frac{p_3}{\ddots \frac{p_n}{q_{n-1} + \frac{p_n}{q_n + \ddots}}}}}$$

以下では、この連分数を下記のような記法で表す。

$$q_0 + \left| \frac{p_1}{q_1} \right| + \left| \frac{p_2}{q_2} \right| + \cdots + \left| \frac{p_n}{q_n} \right| + \cdots$$

この記法での連分数の例を示す。

$$\begin{aligned}\sqrt{23} &= 4 + \frac{1}{1} + \frac{1}{3} + \frac{1}{1} + \frac{1}{8} + \frac{1}{1} + \dots \\ \tan(z) &= \frac{z}{1} - \frac{z^2}{3} - \frac{z^2}{5} - \frac{z^2}{7} - \frac{z^2}{9} - \dots \\ \exp(z) &= 1 + \frac{z}{1} - \frac{z}{2} - \frac{z}{z-3} + \frac{2z}{z-4} + \frac{3z}{z-5} + \dots\end{aligned}$$

### 2.1.2 連分数の用語の定義

分子 ( $p_k$ ) がすべて 1 となるような連分数を正則連分数とよぶ。また、有限で終わる連分数を有限連分数とよび、そうでないものを無限連分数とよぶ。また分母の値が循環する連分数を循環連分数とよぶ。

定理 1 有理数は有限正則連分数で表される。また有限正則連分数は有理数になる [2]。

### 2.1.3 有限正則連分数の性質

実数  $\alpha$  を正則連分数

$$\alpha = q_0 + \frac{1}{q_1} + \frac{1}{q_2} + \dots + \frac{1}{q_n} + \frac{1}{q_{n+1}} + \dots$$

を用いて表したとき、この式を第  $n$  項で打ち切った式を

$$q_0 + \frac{1}{q_1} + \frac{1}{q_2} + \dots + \frac{1}{q_n}$$

とする。この式を既約分数に変形した  $\frac{P_n}{Q_n}$  を  $\alpha$  の連分数による  $n$  次近似分数とよぶ。

定理 2  $P_0 = q_0$ ,  $Q_0 = 1$ ,  $P_{-1} = 1$ ,  $Q_{-1} = 0$  とすると近似分数の分母、分子である  $P_n$  と  $Q_n$  は以下の漸化式を満たす [3]。

$$\begin{cases} P_n = q_n P_{n-1} + P_{n-2} \\ Q_n = q_n Q_{n-1} + Q_{n-2} \end{cases} \quad (n = 1, 2, 3, \dots)$$

故に  $P_n$ ,  $Q_n$  を漸化式を行列を用いて表記すると

$$\begin{aligned}\begin{pmatrix} P_n & Q_n \\ P_{n-1} & Q_{n-1} \end{pmatrix} &= \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} P_{n-1} & Q_{n-1} \\ P_{n-2} & Q_{n-2} \end{pmatrix} \\ &= \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \dots \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\end{aligned}$$

となる。この式を用いることで効率よく計算することができる。

### 2.1.4 $\sqrt{d}$ の正則連分数展開

**定理 3**  $d$  を平方数でない整数とするとき  $\sqrt{d}$  の正則連分数展開は以下のようにして得られる [4].

$S_0 = 0, T_0 = 1, q_0 = [\sqrt{d}]$  として漸化式

$$S_{k+1} = a_k T_k - S_k, \quad T_{k+1} = \frac{d - S_{k+1}^2}{T_k}$$

$$q_{k+1} = \left[ \frac{S_{k+1} + \sqrt{d}}{T_{k+1}} \right]$$

を用いて順次  $q_{k+1}$  を定めていくと  $\sqrt{d}$  の連分数表示は

$$\sqrt{d} = q_0 + \frac{1}{\left| \frac{1}{q_1} \right|} + \frac{1}{\left| \frac{1}{q_2} \right|} + \cdots + \frac{1}{\left| \frac{1}{q_{k-1}} \right|} + \frac{1}{\left| \frac{1}{q_k} \right|} + \cdots$$

と表すことができる.

ここで  $T_{k+1}$  と  $q_{k+1}$  を求めるのに除算を行っているが,  $d - S_{k+1}^2$  は  $T_k$  で必ず割り切れることがわかっている. また,  $[\sqrt{d}] = q_0$  を用いて  $q_{k+1} = \left[ \frac{S_{k+1} + q_0}{T_{k+1}} \right]$  となることも示される. よって  $\sqrt{d}$  の正則連分数展開は整数の計算のみで可能となる.

**定理 4**  $\sqrt{d}$  は次のような連分数となる.

$$\sqrt{d} = q_0 + \frac{1}{\left| \frac{1}{q_1} \right|} + \frac{1}{\left| \frac{1}{q_2} \right|} + \cdots + \frac{1}{\left| \frac{1}{q_{n-1}} \right|} + \frac{1}{\left| \frac{1}{2q_0} \right|} + \frac{1}{\left| \frac{1}{q_1} \right|} + \frac{1}{\left| \frac{1}{q_2} \right|} + \cdots \quad (1)$$

このような分母の値  $q_1$  から  $2q_0$  が循環する連分数を循環連分数と呼ぶ.

例)  $\sqrt{23}$  を連分数で表した場合

$$\sqrt{23} = 4 + \frac{1}{\left| \frac{1}{1} \right|} + \frac{1}{\left| \frac{1}{3} \right|} + \frac{1}{\left| \frac{1}{1} \right|} + \frac{1}{\left| \frac{1}{8} \right|} + \frac{1}{\left| \frac{1}{1} \right|} + \frac{1}{\left| \frac{1}{3} \right|} + \frac{1}{\left| \frac{1}{1} \right|} + \frac{1}{\left| \frac{1}{8} \right|} + \cdots$$

となり, 分母の値が 1, 3, 1, 8 と循環していることがわかり, このときの周期は 4 となる.

故に  $\sqrt{d} + [\sqrt{d}]$  を連分数で表すと初項から循環するような形となる.

例)  $\sqrt{23} + [\sqrt{23}]$  を連分数で表した場合

$$\sqrt{23} + [\sqrt{23}] = 8 + \frac{1}{\left| \frac{1}{1} \right|} + \frac{1}{\left| \frac{1}{3} \right|} + \frac{1}{\left| \frac{1}{1} \right|} + \frac{1}{\left| \frac{1}{8} \right|} + \frac{1}{\left| \frac{1}{1} \right|} + \frac{1}{\left| \frac{1}{3} \right|} + \frac{1}{\left| \frac{1}{1} \right|} + \frac{1}{\left| \frac{1}{8} \right|} + \cdots$$

となり, 初項から 8, 1, 3, 1 と循環するようになる.

一般に以下の形になる.

$$\sqrt{d} + [\sqrt{d}] = 2q_0 + \frac{1}{q_1} + \cdots + \frac{1}{q_{n-1}} + \frac{1}{2q_0} + \frac{1}{q_1} + \cdots \quad (2)$$

以下, (1)の形でなく(2)の形の連分数を扱う. また, 連分数の最小周期を  $N$  とする. 例えば  $\sqrt{23}$  のとき  $N = 4$  である. (2)の形になれば,  $N = n$  となる.

### 2.1.5 近似分数との誤差

よく知られているように次の定理が成立する.

**定理 5**  $d$  を平方数でない整数としたとき  $\sqrt{d}$  の  $n$  次近似分数を  $\frac{P_n}{Q_n}$  とすると

$$\left| \sqrt{d} - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n^2}$$

である [2].

## 2.2 誤差評価

一周期を計算した行列

$$A = \begin{pmatrix} q_{N-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_{N-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 2q_0 & 1 \\ 1 & 0 \end{pmatrix}$$

を  $\begin{pmatrix} p & q \\ p' & q' \end{pmatrix}$  とおく.

このとき行列  $A$  の 2 つの固有値は

$$\alpha = \frac{p+q'}{2} + q\sqrt{d} \quad \beta = \frac{p+q'}{2} - q\sqrt{d}$$

となる. また,  $\alpha > 1 > \beta > -1$  となることに注意する.

**定理 6**  $m$  を正の整数とするとき

$$\left| (\sqrt{d} + [\sqrt{d}]) - \frac{P_{mN-1}}{Q_{mN-1}} \right| = \left| \frac{2\sqrt{d} \left(\frac{\beta}{\alpha}\right)^m}{1 - \left(\frac{\beta}{\alpha}\right)^m} \right|$$

が成り立つ.

## ■証明

$\alpha_0 = \sqrt{d} + [\sqrt{d}]$ ,  $\beta_0 = \sqrt{d} - [\sqrt{d}]$  とおく.

このとき対角化を用いて  $A^m$  を求めると

$$A^m = \begin{pmatrix} \alpha_0 \alpha^m - \beta_0 \beta^m & \alpha^m - \beta^m \\ \beta_0 (\beta^m - \alpha^m) & \alpha_0 \beta^m - \beta_0 \alpha^m \end{pmatrix}$$

よって  $\sqrt{d} + [\sqrt{d}]$  の連分数による  $mN - 1$  次近似分数は

$$\frac{P_{mN-1}}{Q_{mN-1}} = \frac{\alpha_0 \alpha^m - \beta_0 \beta^m}{\alpha^m - \beta^m}$$

となる.

故に, この値と  $\sqrt{d} + [\sqrt{d}]$  との誤差は以下のようにになる.

$$\begin{aligned} \left| (\sqrt{d} + [\sqrt{d}]) - \frac{P_{mN-1}}{Q_{mN-1}} \right| &= \left| \alpha_0 - \frac{\alpha_0 \alpha^m - \beta_0 \beta^m}{\alpha^m - \beta^m} \right| \\ &= \left| \frac{(\alpha_0 - \beta_0) \beta^m}{\alpha^m - \beta^m} \right| \\ &= \left| \frac{(\alpha_0 - \beta_0) \left(\frac{\beta}{\alpha}\right)^m}{1 - \left(\frac{\beta}{\alpha}\right)^m} \right| \\ &= \left| \frac{2\sqrt{d} \left(\frac{\beta}{\alpha}\right)^m}{1 - \left(\frac{\beta}{\alpha}\right)^m} \right| \end{aligned}$$

(証明終)

$\sqrt{d}$  の近似分数  $\frac{P_n}{Q_n}$  の  $n = mN - 1$  を  $\sqrt{d}$  の桁数  $M$  まで求めることを考える。

$$\left| (\sqrt{d} + [\sqrt{d}]) - \frac{P_{mN-1}}{Q_{mN-1}} \right| = \left| \frac{2\sqrt{d} \left(\frac{\beta}{\alpha}\right)^m}{1 - \left(\frac{\beta}{\alpha}\right)^m} \right|$$

なので

$$\left| \frac{2\sqrt{d} \left(\frac{\beta}{\alpha}\right)^m}{1 - \left(\frac{\beta}{\alpha}\right)^m} \right| \leq 10^{-M}$$

とすればよい。

この式を  $m$  について解くと

$$m \geq \frac{M - \log_{10}(2\sqrt{d} - 10^{-M})}{\log_{10} \alpha - \log_{10} \beta}$$

この  $m$  に対し、 $A^m = \begin{pmatrix} p & q \\ p' & q' \end{pmatrix}^m$  を計算することで指定した桁数の近似値を求めることができる。また、この  $m$  をべき乗数とよぶことにする。

### 2.3 近似値の算出方法

連分数の周期が  $N$  である平方根の近似値を求める手順を以下に示す。

1.  $\sqrt{d} + [\sqrt{d}]$  を一周分だけ連分数展開する。

2. 一周分の行列の積

$$A = \begin{pmatrix} q_{N-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_{N-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 2q_0 & 1 \\ 1 & 0 \end{pmatrix}$$

とおく。つまり

$$A = \begin{pmatrix} P_{N-1} & Q_{N-1} \\ P_{N-2} & Q_{N-2} \end{pmatrix}$$

である。この  $A$  を計算する。

3. 一周分を計算した行列  $A$  を  $m$  乗 ( $m$  は  $\sqrt{d}$  の近似値の桁数から決まる整数)

4.  $A^m$  の  $[1, 1]$  成分 ( $P_{mN-1}$ ) を  $[2, 1]$  成分 ( $Q_{mN-1}$ ) で除算し、 $[\sqrt{d}]$  を引く。

この手法を用いると、手順4にある除算1回で近似値を求められる。

### 3 漸化式を用いた近似値の求め方

#### 3.1 漸化式について

$a$  を正の整数とし,  $R_0 = a$ ,  $S_0 = 1$  として  $R_n$  と  $S_n$  を以下の漸化式で定める.

$$\begin{cases} R_n = aR_{n-1} + dS_{n-1} \\ S_n = R_{n-1} + aS_{n-1} \end{cases} \quad (n = 1, 2, 3, \dots)$$

この漸化式を行列を用いて表記すると

$$\begin{aligned} \begin{pmatrix} R_n \\ S_n \end{pmatrix} &= \begin{pmatrix} a & d \\ 1 & a \end{pmatrix} \begin{pmatrix} R_{n-1} \\ S_{n-1} \end{pmatrix} \\ &= \begin{pmatrix} a & d \\ 1 & a \end{pmatrix} \begin{pmatrix} a & d \\ 1 & a \end{pmatrix} \begin{pmatrix} R_{n-2} \\ S_{n-2} \end{pmatrix} \\ &= \begin{pmatrix} a & d \\ 1 & a \end{pmatrix}^n \begin{pmatrix} a \\ 1 \end{pmatrix} \end{aligned}$$

#### 3.2 誤差評価

$$A = \begin{pmatrix} a & d \\ 1 & a \end{pmatrix}$$

とおく. このとき行列  $A$  の 2 つの固有値は

$$\alpha = a + \sqrt{d}, \quad \beta = a - \sqrt{d}$$

となる.

定理 7

$$\left| \sqrt{d} - \frac{R_n}{S_n} \right| = \left| \frac{2\sqrt{d} \left( \frac{\beta}{\alpha} \right)^{n+1}}{1 - \left( \frac{\beta}{\alpha} \right)^{n+1}} \right|$$

が成り立つ.

■証明

対角化を用いて  $A^n$  を求めると

$$A^n = \begin{pmatrix} \sqrt{d}\alpha^n + \sqrt{d}\beta^n & d\alpha^n - d\beta^n \\ \alpha^n - \beta^n & \sqrt{d}\alpha^n + \sqrt{d}\beta^n \end{pmatrix}$$

なので

$$\begin{aligned} \begin{pmatrix} R_n \\ S_n \end{pmatrix} &= A^n \begin{pmatrix} a \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{d}\alpha^n + \sqrt{d}\beta^n & d\alpha^n - d\beta^n \\ \alpha^n - \beta^n & \sqrt{d}\alpha^n + \sqrt{d}\beta^n \end{pmatrix} \begin{pmatrix} a \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{d}\{(a + \sqrt{d})\alpha^n + (a - \sqrt{d})\beta^n\} \\ (a + \sqrt{d})\alpha^n - (a - \sqrt{d})\beta^n \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{d}(\alpha^{n+1} + \beta^{n+1}) \\ \alpha^{n+1} - \beta^{n+1} \end{pmatrix} \end{aligned}$$

よって  $\sqrt{d}$  の近似分数は

$$\begin{aligned} \frac{R_n}{S_n} &= \frac{\sqrt{d}(\alpha^{n+1} + \beta^{n+1})}{\alpha^{n+1} - \beta^{n+1}} \\ &= \frac{\sqrt{d}\left\{1 + \left(\frac{\beta}{\alpha}\right)^{n+1}\right\}}{1 - \left(\frac{\beta}{\alpha}\right)^{n+1}} \end{aligned}$$

この近似分数  $\frac{R_n}{S_n}$  と  $\sqrt{d}$  との誤差は

$$\begin{aligned} \left| \sqrt{d} - \frac{R_n}{S_n} \right| &= \left| \sqrt{d} - \frac{\sqrt{d}\left\{1 + \left(\frac{\beta}{\alpha}\right)^{n+1}\right\}}{1 - \left(\frac{\beta}{\alpha}\right)^{n+1}} \right| \\ &= \left| \frac{2\sqrt{d}\left(\frac{\beta}{\alpha}\right)^{n+1}}{1 - \left(\frac{\beta}{\alpha}\right)^{n+1}} \right| \end{aligned}$$

(証明終)

この定理7より以下の系が導かれる.

系  $\sqrt{d}$  の  $n$  次近似分数を  $\frac{R_n}{S_n}$  とするとき

$$\lim_{n \rightarrow \infty} \frac{R_n}{S_n} = \sqrt{d}$$

が成り立つ.

■証明

$$\lim_{n \rightarrow \infty} \left(\frac{\beta}{\alpha}\right)^{n+1} = 0 \text{ より}$$

$$\lim_{n \rightarrow \infty} \frac{2\sqrt{d} \left(\frac{\beta}{\alpha}\right)^{n+1}}{1 - \left(\frac{\beta}{\alpha}\right)^{n+1}} = 0$$

故に

$$\lim_{n \rightarrow \infty} \frac{R_n}{S_n} = \sqrt{d}$$

(証明終)

定理7の右辺において,  $a$  が  $\sqrt{d}$  に近いとき  $\left|\frac{\beta}{\alpha}\right| < 1$  がより小さい値となる. したがって  $a$  は  $[\sqrt{d}]$  または  $[\sqrt{d}] + 1$  のいずれかで,  $\sqrt{d}$  に近い値を用いる.

以上の理由により,  $\frac{R_n}{S_n}$  は  $\sqrt{d}$  の近似分数になることが示された.

$\sqrt{d}$  の近似分数  $\frac{R_n}{S_n}$  の  $n$  を  $\sqrt{d}$  の桁数  $M$  まで求めることを考える.

$$\left| \sqrt{d} - \frac{R_n}{S_n} \right| = \left| \frac{2\sqrt{d} \left(\frac{\beta}{\alpha}\right)^{n+1}}{1 - \left(\frac{\beta}{\alpha}\right)^{n+1}} \right|$$

なので

$$\frac{2\sqrt{d} \left(\frac{\beta}{\alpha}\right)^{n+1}}{1 - \left(\frac{\beta}{\alpha}\right)^{n+1}} \leq 10^{-M}$$

とすればよい.

この式の  $n$  を  $M$  について解くと

$$n \geq \frac{M + \log_{10}(2\sqrt{d} + 10^{-M})}{\log_{10} \alpha - \log_{10} \beta}$$

この  $n$  に対し  $\begin{pmatrix} R_n \\ S_n \end{pmatrix} = \begin{pmatrix} a & d \\ 1 & a \end{pmatrix}^n \begin{pmatrix} a \\ 1 \end{pmatrix}$  を計算することで近似値の桁数を一桁ずつ指定することができる. また, この  $n$  をべき乗数とよぶことにする.

## 4 ニュートン法を用いた近似値の求め方

### 4.1 ニュートン法について

$\sqrt{d}$  のときニュートン法を用いて近似値を求めるには次の式を用いる。

$$a_{n-1} = \frac{1}{2} \left( a_n + \frac{d}{a_n} \right)$$

$a_n = \frac{U_n}{V_n}$  において整理すると

$$\frac{U_{n+1}}{V_{n+1}} = \frac{1}{2} \left( \frac{U_n^2 + dV_n^2}{U_n V_n} \right)$$

この式より以下の漸化式が得られる。ただし初期値は  $U_0 = [\sqrt{d}]$ ,  $V_0 = 1$  をとるとよい。

$$\begin{cases} U_{n+1} = U_n^2 + dV_n^2 \\ V_{n+1} = 2U_n V_n \end{cases} \quad (n = 1, 2, 3, \dots)$$

この手法においても  $U_{n+1}$ ,  $V_{n+1}$  は整数のみで計算することができ、一回のみの除算で近似値を計算できる。

## 5 数値実験

これまでに述べた3つの手法をそれぞれ Risa/Asir で実装し、PARI/GP との比較を行った。

### 5.1 計測環境

今回、計測に用いた環境を下記に示す。

OS : Fedora 20 (64bit)  
 CPU : Intel Core i5-4440 3.1GHz  
 メモリ : 8GB  
 Risa/Asir ver 20140731  
 PARI/GP ver 2.7.1

## 5.2 計測結果

$\sqrt{d}$ の近似値をそれぞれの手法で5万桁計算した結果を表1に、連分数、漸化式、ニュートン法を用いた手法の計算時間の内訳を表2~4に示す。

表1から、PARI/GPと比べて連分数では約5.0倍、漸化式では約3.3倍、ニュートン法では約3.8倍の速度で近似値を求めることができた。しかし連分数を用いた手法では、連分数の一周期が長くなると計算時間が増えるという欠点があり、 $\sqrt{123456789}$ では、ほかの $d$ の値に比べて約27倍の時間がかかっている。表2より $\sqrt{123456789}$ の周期は8164となり、べき乗数計算に多くの時間がかかっていることがわかる。さらに周期が長い $\sqrt{1234567890123456789}$ では、1時間以上計算しても、べき乗数を出すことはできなかった。また連分数の周期は $d$ の値からは簡単に計算することはできない。

漸化式、ニュートン法を用いた手法では、 $d$ やべき乗数の値によらず、一定の速度で近似値を求めることができた。

また、 $\sqrt{23}$ の近似値を68382桁と68383桁求めた結果を表5に記す。68382桁というのはニュートン法を16回くり返したときに求められた桁数であるが、例えば近似値を68383桁求めたいといった場合にニュートン法は二次収束のため、くり返し回数が1回増えてしまい、計算時間も約2倍多くなる。しかし、漸化式を用いた手法は桁数の指定が1桁ずつ可能になってるため余計な計算を行わず、ニュートン法よりも安定した速度で近似値が計算できる。

表 1:  $\sqrt{d}$ の近似値を5万桁計算した時間 (msec)

$d$	連分数	漸化式	ニュートン法	PARI/GP
23	37	41	49	197
13126	39	58	56	195
123456788	39	69	51	199
123456789	1017	65	53	203
123456790	37	69	50	204
1234567890123456789	×	66	56	203

表 2: 連分数の内訳

$d$	周期	べき乗数	計算時間 (msec)			
			べき乗数計算	$R_n, S_n$ 計算	除算	合計
23	4	16667	0	21	16	37
13126	262	233	1	22	16	39
123456788	334	161	2	22	15	39
123456789	8164	8	976	26	15	1017
123456790	4	3126	0	24	16	37
1234567890123456789	18794642	×	×	×	×	×

表 3: 漸化式の内訳

$d$	べき乗数	計算時間 (msec)			
		べき乗数計算	$R_n, S_n$ 計算	除算	合計
23	29743	0	25	16	41
13126	18341	0	42	16	58
123456788	11503	0	52	16	68
123456789	11503	0	50	15	65
123456790	11503	0	53	15	68

表 4: ニュートン法の内訳

$d$	繰返し回数	計算時間 (msec)		
		$U_n, V_n$ 計算	除算	合計
23	16	33	16	49
13126	15	41	15	56
123456788	14	35	16	51
123456789	14	37	16	53
123456790	14	35	15	50

表 5:  $\sqrt{23}$  のときの各桁数の比較

	連分数		漸化式		ニュートン法	
	べき乗数	msec	べき乗数	msec	繰返し回数	msec
68382 桁	22795	56	40678	67	16	61
68383 桁	22795	56	40679	68	17	122

## 6 まとめ

誤差評価を含めた平方根の近似値計算を Risa/Asir で実装し, PARI/GP より短時間で  $\sqrt{d}$  の任意精度を求めることができた。(5 万桁で約 1/5 の計算時間)

連分数法では  $\sqrt{d}$  の周期が小さい (3 桁以下) のときは最速に近似値を計算することができるが, 周期が長いと計算に時間がかかってしまう。(一般に連分数の周期は  $d$  から簡単に計算できない)

漸化式法は  $d$  や求めたい桁数によらず, 安定した速度で近似値を求めることができたが, 必ずしも最速に計算できるわけではなかった。

ニュートン法は 2 次収束であるため, 求めたい桁数により計算時間に段差が発生することとなった。

## 7 課題

今後の課題として、漸化式を用いた手法の初期値を、連分数で作った近似分数にすることでより高速に近似値の計算が可能になると思われる。その際に、連分数の周期をある程度の長さで打ち切ることで、連分数の欠点を回避できる。

## 参考文献

- [1] Isao Makino, Takeshi Aoyama, The arbitrary precision calculation of logarithms with continued fraction expansion, 京都大学数理解析研究所講究録 No.1138, pp.240-246, 2000/04.
- [2] 木田祐司, 牧野潔夫, UBASIC によるコンピュータ整数論, 1994.
- [3] A.N. Khvanskii, The application of continued fractions and their generalizations to problem in approximation theory, P. Noordhoff, 1963.
- [4] 和田秀夫, 数の世界-整数論への道, 岩波書店, 1981.