プログラムのページ（担当　高　橋　　理）

75-04　実2次数体の類数の計算

片　山　　茂*

実2次数体のイデアル類の数とその代表を求めるプログラムについてのべる．これは筆者のプログラム[1]を和田[2]によって改良したものである．

計算の根拠を簡単にのべると，実2次数体のイデアル類の対等は実2次無理数の対等（モジュラー変換でむすばれる）に帰着され，実2次無理数は簡約された2次無理数に対等になる．また判別式を与えると，それに属する簡約された2次無理数は有限個しかないので，類数は簡約された2次無理数のうち対等でないものの個数で決まる．

1.　〈X, Y, Z〉の決定

M(≠1) を平方因数のない自然数として，2次体 $Q(\sqrt{M})$ の判別式を MD とすると

$M\equiv 1 \pmod 4$ のとき　$MD=M$,

$M\not\equiv 1 \pmod 4$ のとき　$MD=4M$.

MDに属する簡約された2次無理数 ω の代りにその満足する方程式

$$(KC\,1)\omega^2+(KC\,2)\omega+(KC\,3)=0$$

の整係数の組 〈KC 1, KC 2, KC 3〉 を考える，これらは，ω の定義：$1<\omega$，$-1<\omega'<0$ (ω' は ω の共役数) から次の条件(0)～(iv)をみたす，逆にこのような整数の組 〈KC 1, KC 2, KC 3〉 から一つの MD に属する簡約された2次無理数がきまる．

$$KC\,1>0,\ KC\,2<0,\ KC\,3<0 \qquad (0)$$

$$\left.\begin{array}{l}|KC\,2|\leqq[\sqrt{MD}],\\ KC\,2:\text{奇数(偶数)} \Leftrightarrow MD:\text{奇数(偶数)}\end{array}\right\} \quad (i)$$

$$KC\,1L=\left[\frac{-|KC\,2|+[\sqrt{MD}]}{2}\right]+1,$$

$$KC\,1U=\left[\frac{|KC\,2|+[\sqrt{MD}]}{2}\right]$$

とおくとき，

$$KC\,1L\leqq KC\,1\leqq KC\,1U \qquad (ii)$$

$$ID=\left[\frac{MD-(KC\,2)^2}{4}\right]$$

とおくとき，

$$(KC\,1)|KC\,3|=ID \qquad (iii)$$

$$(KC\,1, KC\,2, KC\,3)=1 \qquad (iv)$$

(iv)はMの条件から，また(ii)，(iii)から $KC\,1L\leqq|KC\,3|\leqq KC\,1U$ がでる．

X=KC 1，Y=KC 2，Z=KC 3 とおく，先ずYは(i)からきめる，Xは(ii)，(iii)によるが ID を小さい素数から順に割り，その因数となるものP，その重複度Eを求め，ID の素因数分解：

$$ID=P(1)^{E(1)}*\cdots*P(JZ)^{E(JZ)}$$

を作る（**流れ図-1**）．次にその約数

$$G(JZ)=P(1)^{F(1)}*\cdots*P(JZ)^{F(JZ)}$$

$$0\leqq F(L)\leqq E(L)$$

をその指数の $(0,\cdots,0,1),(0,\cdots,0,2)\cdots$ なる辞書式順

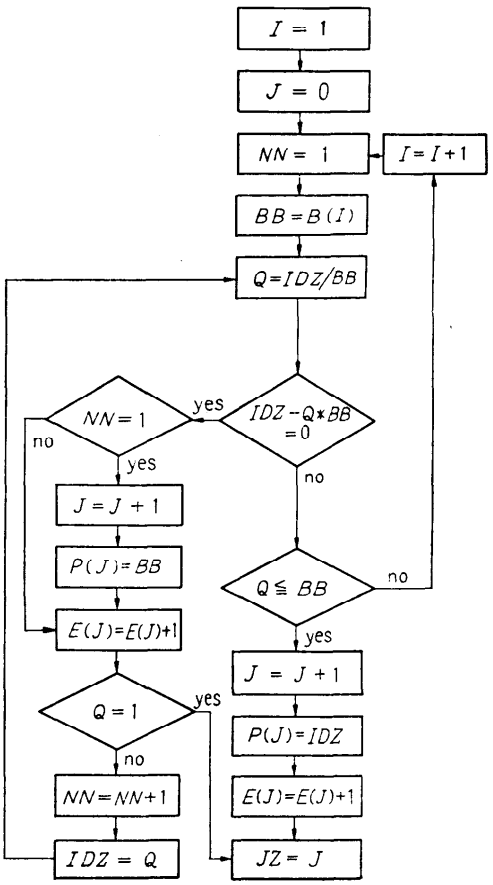

図-1　流れ図（素因数分解）

* 鳥取大学教育学部

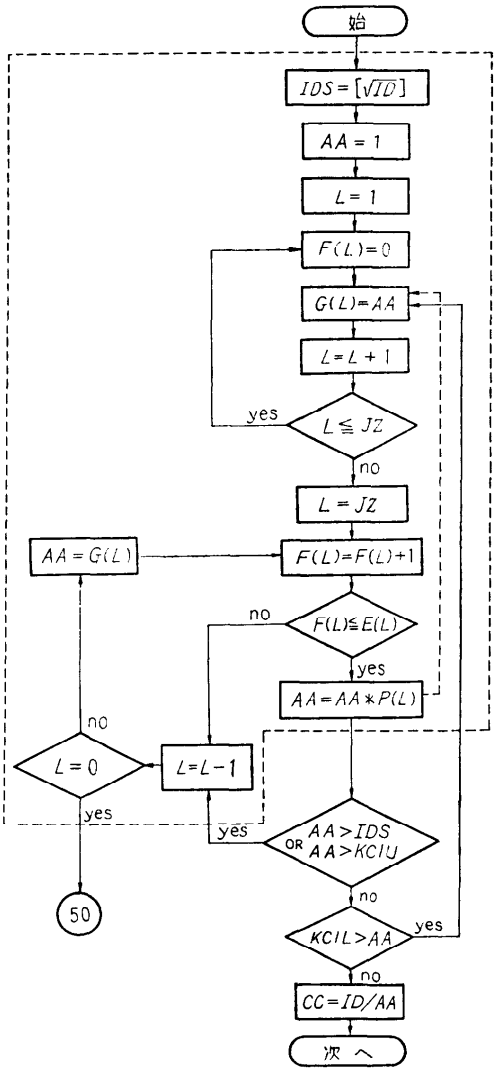

図-2　流れ図（因数の選出）

序ですべてとり出し（**流れ図-2** で破線の内部と破線矢），条件(ii)と X≦[√ID] に適しないものを捨てる（流れ図-2で破線の外部），Zは(iii)からきまる．

KC1L=1 のときは X=1, Z=ID が条件をみたすが，これは別に扱うようにしてある．

なお，筆者のプログラム[1]では，範囲(i)の各Y(小さい方から)に対し，範囲(ii)のX(小さい方から)でIDを割り切るもの(商がZ)のみ選び〈X, Y, Z〉を決めた．

2. 〈X, Y, Z〉の対等

ω' が ω に対等であれば，ω の連分数展開で必ず ω' が表われるから，対等でないものの選出には，$\omega_1\langle X, Y, Z\rangle$ が一つ決まったら，$\omega_1\langle X, Y, Z\rangle$ の連分数展開（筆者のプログラム[4]参照）から，対等な $\omega'\langle X', Y', Z'\rangle$ をすべて求め，この集合を S_1 としてこれらを配列〈MA, MB, MC〉に記憶する，この集合を $\boldsymbol{S}$ とする．次に決定された $\omega_2\langle X'', Y'', Z''\rangle$ について $\boldsymbol{S}$ の元と対等かどうかを〈X, Y, Z〉の一致，不一致で判定する．(イ) $\boldsymbol{S}$のどれかの元と一致すれば，ω_2 は捨てる，(ロ) $\boldsymbol{S}$ のすべての元と一致しなければ，$\omega_2\langle X'', Y'', Z''\rangle$ に対等な $\omega\langle X, Y, Z\rangle$ を ω_2 の連分数展開から求め，これらを集合 S_2 とし配列〈MA, MB, MC〉に追加記憶する，この $S_1 \cup S_2$ をあらためて $\boldsymbol{S}$ とする．

このような手順を続けて，$\omega\langle X, Y, Z\rangle$ の生成が尽きたとき終了する（subroutine ISR 参照）．

集合 S_i の個数が類数で，このカウンタをCLNとしてある．また各 S_i の元を一つ宛プリントさせてあるが，これから直ちに代表イデアルが計算できる[3]．

なお，subroutine PRSB は'エラトステネスのふるい'の方法で奇素数を生成するもので，それを配列Bに記憶する[5]．

3. テスト結果

プログラム[1]（以下「旧」）と本稿のプログラム（以下「新」）との比較，使用計算機は FACOM 230-75（京都大学）である．

比較内容	旧	新
TOTAL CPU TIME を 200100MS として MD が 80809 以上の $4n+1$ の形の素数であるものの計算できる個数	82021 までの 59 個	82141 までの 63 個
M=82, 12037, 2776817 の3数に対し別表の結果を出力する時間	TOTAL CPU TIME	
	11900MS	4300MS

「旧」は〈X, Y, Z〉の決定の部分のプログラムは「新」より簡単である，また桁数の小さい範囲では計算時間はあまり変らないが，桁数が大きくなると「新」の能率がきわめて良いことがわかる．

(注 1)　Bの寸法は $\sqrt{M}$ を考慮してきめるべきであるが，ここでは一応2～10193の素数1252個を記憶させてある．

(注 2)　MA, MB, MC の寸法は，集合 $\boldsymbol{S}$ の個数によるので配列超過のチェックは IN の値による（ISR 第20行）．MD が $4n+1$ の形の素数であるものの 228773 までの類数計算では寸法 5000 で十分であった．なお計算例の 12037, 2776817 の IN の最終値は

```
      C   COMPUTATION OF CLASS NUMBER
      C   OF REAL QUADRATIC NUMBER FIELD
      C   MAIN PROGRAM
    1       INTEGER MA(5000),MB(5000),MC(5000),
           1P(100),E(100),F(100),G(100),
           2AA,CC,CLN,Q,B(1252),BB
    2       COMMON B,MA,MB,MC,CLN,KK,IN,MDS,IC2
    3       CALL PRSB
    4   10  READ(5,100) M
    5   100 FORMAT(I10)
    6       IF(M.EQ.0) STOP
    7       IF(MOD(M,4).EQ.1) GO TO 400
    8       MD=4*M
    9       KIGUZ=2
   10       GO TO 401
   11   400 MD=M
   12       KIGUZ=1
   13   401 MDS=SQRT(FLOAT(MD))+0.1
   14       MA(1)=0
   15       MB(1)=0
   16       MC(1)=0
   17       CLN=0
   18       IN=1
   19       KK=0
   20       DO 50 IC2=KIGUZ,MDS,2
   21       KC1L=(MDS-IC2)/2+1
   22       KC1U=(MDS+IC2)/2
   23       ID=(MD-IC2*IC2)/4
   24       IDZ=ID
   25       IF(KC1L.NE.1) GO TO 26
   26       CALL ISR(1,ID)
   27       CALL ISR(ID,1)
      C   FACTORIZATION OF IDZ
   28   26  I=1
   29       J=0
   30       DO 30 N=1,100
   31   30  E(N)=0
   32   1   NN=1
   33       BB=B(I)
   34   2   Q=IDZ/BB
   35       IF(IDZ-Q*BB.NE.0) GO TO 4
   36       IF(NN.NE.1) GO TO 3
   37       J=J+1
   38       IF(J.GE.100) STOP 777
   39       P(J)=BB
   40   3   E(J)=E(J)+1
   41       IF(Q.EQ.1) GO TO 6
   42       NN=NN+1
   43       IDZ=Q
   44       GO TO 2
   45   4   IF(Q.LE.BB) GO TO 5
   46       I=I+1
   47       GO TO 1
   48   5   J=J+1
   49       IF(J.GE.100) STOP 7777
   50       P(J)=IDZ
   51       E(J)=E(J)+1
   52   6   JZ=J
      C   SELECTION OF FACTORS

   53       IDS=SQRT(FLOAT(ID))+0.1
   54       AA=1
   55       L=1
   56   11  F(L)=0
   57   22  G(L)=AA
   58       L=L+1
   59       IF(L.LE.JZ) GO TO 11
   60       L=JZ
   61   12  F(L)=F(L)+1
   62       IF(F(L).LE.E(L)) GO TO 14
   63   13  L=L-1
   64       IF(L.EQ.0) GO TO 50
   65       AA=G(L)
   66       GO TO 12
   67   14  AA=AA*P(L)
   68       IF(AA.GT.IDS.OR.AA.GT.KC1U) GO TO 13
   69       IF(KC1L.GT.AA) GO TO 22
   70       CC=ID/AA
   71       CALL ISR(AA,CC)
   72       IF(AA-CC.NE.0) CALL ISR(CC,AA)
   73       GO TO 22
   74   50  CONTINUE
   75       WRITE(6,203) M,CLN
   76   203 FORMAT(1H0,7X,7HNUMBER=,I10,
           12X,13HCLASS NUMBER=,I10)
   77       GO TO 10
   78       END
```

```
    1       SUBROUTINE ISR(X,Z)
    2       INTEGER MA(5000),MB(5000),MC(5000),
           1CLN,X,Z,B(1252)
    3       COMMON B,MA,MB,MC,CLN,KK,IN,MDS,IC2
    4       KC1=X
    5       KC2=IC2
    6       KC3=Z
    7       LC1=KC1
    8       LC2=KC2
    9       LC3=KC3
   10       DO 66 I=1,IN
   11       IF(LC1-MA(I)) 66,64,66
   12   64  IF(LC2-MB(I)) 66,65,66
   13   65  IF(LC3-MC(I)) 66,40,66
   14   66  CONTINUE
   15       CLN=CLN+1
   16       WRITE(6,202) LC1,LC2,LC3
   17   202 FORMAT(1H ,3I15)
   18   67  KK=KK+1
   19       IN=KK
   20       IF(IN.GE.5000) STOP 77777
   21       MA(IN)=KC1
   22       MB(IN)=KC2
   23       MC(IN)=KC3
   24       MDK=MDS-KC2
   25       KMK=2*KC1
   26       N=MDK/KMK
   27       KKC1=-((KC1*N+KC2)*N+KC3)
   28       KKC2=-KMK*N-KC2
   29       KKC3=-KC1
   30       IF(LC1-KKC1) 76,74,76
   31   74  IF(LC2-KKC2) 76,75,76
   32   75  IF(LC3-KKC3) 76,40,76
   33   76  KC1=KKC1
   34       KC2=KKC2
   35       KC3=KKC3
   36       GO TO 67
   37   40  RETURN
   38       END
```

```
          9              -2              -9
          6              -8             -11
         11              -8              -6
          1             -18              -1

 NUMBER=         82  CLASS NUMBER=           4
         51             -35             -53

 NUMBER=      12037  CLASS NUMBER=           1
        812             -55            -854
        826             -69            -839
        839             -69            -826

 NUMBER=    2776817  CLASS NUMBER=           3
```

それぞれ 53, 1093 である.

(注 3) P, E の寸法は IDZ に関係するが, 当初には確定できないので, 主プログラム 38 行, 49 行で配列超過のチェックをする. F, G の寸法は P, E と同一にする.

参 考 文 献

1) 片山: 実2次数体の類数, 鳥取大学教育学部研究報告, 22-2, pp. 44～54 (1972).
2) 和田: Hecke operators の計算について, 数理解析研究所講究録 155, pp. 3～13 (1971).
3) 高木: 初等整数論講義, 共立出版 (1971).
4) 片山: 実2次数体の基本単数の計算, 情報処理, Vol. 15, No. 2, pp. 154～156 (1974).
5) 片山: 素数の計算, 情報処理, Vol. 15, No. 11, pp. 903～904 (1974).

(昭和49年12月9日受 付)
(昭和50年5月16日再受付)