

プログラムのページ

78-02 実2次数体の類数計算の一工夫

片 山 茂*

実2次数体の類数とその代表イデアルを計算する筆者の方法¹⁾では m が大きいとき配列 MA, MB, MC に不当に多くの番地をあらかじめ用意している。この欠点を除く方法とプログラムを報告する。なおこの方法はイデアル類群の計算²⁾をする際にも都合よいものである。

1. 計算法とプログラム

m を素数の平方で割れない, 1 より大きい自然数とするとき, 実2次数体 $Q(\sqrt{m})$ の類数とは,

[I] $m \equiv 1 \pmod{4}$ のときは,

(1) $1 \leq b \leq [\sqrt{m}]$ かつ奇数,

(2) $\left[\frac{[\sqrt{m}] - b}{2} \right] + 1 \leq a \leq \left[\frac{[\sqrt{m}] + b}{2} \right]$,

(3)** $a \mid \frac{(m-b^2)}{4}$

[II] $m \equiv 1 \pmod{4}$ のときは,

(1') $1 \leq b \leq [\sqrt{m}]$,

(2') $[\sqrt{m}] - b + 1 \leq a \leq [\sqrt{m}] + b$,

(3')** $a \mid (m-b^2)$

をみたす整数の組 (a, b) からの2次無理数

$$\frac{b+\sqrt{m}}{2a} \quad ([I] \text{ のとき}), \quad \frac{b+\sqrt{m}}{a} \quad ([II] \text{ のとき})$$

の集合を S とすると, " S の各元の連分数展開 (以下単に展開という) で独立な部分集合 S_0 "*** の元の個数のことである³⁾。

一般に無理数 ω の展開は

$$\omega = k_0 + \frac{1}{k_1 + \frac{1}{k_2 + \cdots + \frac{1}{k_{n-1} + \frac{1}{\omega_n}}}}$$

で, 整数 k_m は $k_m < \omega_m < k_m + 1$, ω_n を終項という。

特に実2次数体の2次無理数の展開では, 終項に必ず S の元が表われ, S の元の展開は純循環である。

* 鳥取大学教育学部数学教室

** a/x は, a は x の約数

*** "... " とは S_0 の各元の展開の各終項には自身以外の S_0 の元は表われない, また $S-S_0$ の元は S_0 のどれかの元の展開のある終項として表われるような集合のこととする。

$\omega_0 = (b_0 + \sqrt{m})/a_0$ とするとき, 次の終項 ω_1 , すなわち $\omega_0 = k_0 + 1/\omega_1$, $\omega_1 = (b_1 + \sqrt{m})/a_1$ は

$$k_0 = \left[\frac{b_0 + [\sqrt{m}]}{a_0} \right],$$

```

C  COMPUTATION OF CLASS NUMBER
C  OF REAL QUADRATIC NUMBER FIELD
C  MAIN PROGRAM
01  IMPLICIT INTEGER(A-V)
02  INTEGER P(100),E(100),F(100),G(100),
1E(1252),U(300),V(200),U2(300),V2(300)
03  COMMON/AB/5/L3/P,E,F/M3/JZ
1/FB/U,V,U2,V2,CLN/PB/MS
2/FB/M,MCDM
3/G3/IO,C1U,C1L,C2
4/G3/N
5/NE/G
04  CALL PRSB
05 10 READ(5,100) M
06 100 FORMAT(I10)
07  IF(M.EQ.0) STCP
08  DO 99 JJ=1,100
09  F(JJ)=0
10  G(JJ)=0
11  P(JJ)=0
12 99 CONTINUE
13  N=1
14  MS=SQRT(FLOAT(M))
15  MCDM=MCD(M,4)
16  IF(MODM.NE.1) GO TO 400
17  MSS=MS-MCD(MS+1,2)
18  U(1)=1
19  V(1)=0
20  U2(1)=2
21  V2(1)=MSS
22  DO 50 C2=1,MS,2
23  C1L=(MS-C2)/2+1
24  C1U=(MS+C2)/2
25  ID=(M-C2+C2)/4
26  IF(ID.EQ.1) GO TO 50
27  IDZ=ID
28  IF(C1L.NE.1) GO TO 401
29  IDL=ID
30  C2L=C2
31  CALL KETT(IDL,C2L)
32 401 CALL FACTOR(IDZ)
33  CALL SELECT
34 50 CONTINUE
35  CLN=N
36  GO TO 70
37 400 U(1)=1
38  V(1)=0
39  U2(1)=1
40  V2(1)=MS
41  DO 60 C2=1,MS
42  C1L=(MS-C2)+1
43  C1U=MS+C2
44  ID=M-C2+C2
45  IF(ID.EQ.1) GO TO 60
46  IDZ=ID
47  IF(C1L.NE.1) GO TO 402
48  C2LL=C2
49  IDLL=ID
50  CALL KETT(IDLL,C2LL)
51 402 CALL FACTOR(IDZ)

52  CALL SELECT
53  CONTINUE
54  CLN=N
55 70 WRITE(6,201) M,CLN
56 201 FORMAT(1H0,7X,7HNUMBER=,110,
12X,13HCLASS NUMBER=,15)
57  WRITE(6,202)
58 202 FORMAT(1H ,7X,13HIDEAL CLASSES)
59  WRITE(6,203) (U(J),V(J),J=1,CLN)
60 203 FORMAT(1H ,20X,1H(,14,1H,14,3H+))
61  GO TO 10
62  END

```

メインプログラム

```

178      SUBROUTINE KETT(A,B)
179      IMPLICIT INTEGER(A-V)
180      INTEGER U(300),V(300),U2(300),V2(300)
181      COMMON /FB/U,V,U2,V2,CLN/PB/MS
182      1/BB/M,MCDM
183      2/GS/N
184      IF(MODM.NE.1) GO TO 2
185      AZ=2*A
186      GO TO 3
187      2  AZ=A
188      3  BZ=B
189      A1=AZ
190      B1=BZ
191      KZ=(B1+MS)/A1
192      NR=(M-B1*B1)/A1
193      B2=A1*KZ-B1
194      A2=NR+2*B1*KZ-A1*KZ*KZ
195      DO 10 I=1,N
196      IF(U2(I)-A2) 10,11,10
197      IF(V2(I)-B2) 10,12,10
198      CONTINUE
199      IF(AZ-A2) 13,14,13
200      IF(BZ-B2) 13,15,13
201      A1=AZ
202      B1=BZ
203      GO TO 5
204      N=N+1
205      IF(MODM.NE.1) GO TO 400
206      U2(N)=AZ
207      V2(N)=BZ
208      BZZ=(BZ-1)/2
209      V(N)=MOD(BZZ,AZZ)
210      GO TO 12
211      400 U2(N)=AZ
212      U(N)=AZ
213      V2(N)=BZ
214      V(N)=MOD(BZ,AZ)
215      RETURN
216      END

```

サブルーチン

とおくと

$$b_1 = a_0 k_0 - b_0,$$

$$a_1 = 2b_0 k_0 - a_0 k_0^2 + (m - b_0^2)/a_0$$

である。

これらのことから S より S_0 を求めるのにはまず、主類 (単項類) に対して、 $m \equiv 1, \equiv 1 \pmod{4}$ に従って、それぞれ $a_0 = 2(a=1)$, $b_0 = [\sqrt{m}] - \text{MOD}([\sqrt{m}] + 1, 2)$; $a_0 = 1$, $b_0 = [\sqrt{m}]$ として S_0 の第1元とする。これを C_1 とおく。——プログラム第20,21行及び第39,40行。

次に b の順で発生する S の元を展開し、循環節の各終項の (a_1, b_1) を C_1 と比較し、一致することがあれば捨て、一致しなければ S_0 の第2元 C_2 とする。

次の S の元の展開について、同様に比較を C_1, C_2 について行い、いずれかと一致すれば捨て、一致しないとき S_0 の第3元 C_3 とする。このように続けて S_0 が構成されて、その元の個数は類数となる。——プログラム第22行、第41行 DO文。

筆者の前の方法¹⁾では、2次無理数 (a_0, b_0) の代りに、それを満たす2次方程式の係数の組 $\langle X, Y, Z \rangle$ を用いている。従って記憶番地が3個から2個に減り、比較の手数も減っている。また S_0 の構成では、前¹⁾には S_0 に入る各元の展開の循環節のすべての終項に対応する $\langle X, Y, Z \rangle$ までも S_0 に追加しているが、そ

```

NUMBER=      82  CLASS NUMBER=      4
IDEAL CLASSES
( 1, 0+M)
( 9, 1+M)
( 6, 4+M)
( 11, 4+M)

```

```

NUMBER=    32009  CLASS NUMBER=      9
IDEAL CLASSES
( 1, 0+M)
( 86, 9+M)
( 92, 9+M)
( 85, 13+M)
( 92, 13+M)
( 58, 36+M)
( 115, 36+M)
( 43, 9+M)
( 122, 52+M)

```

```

NUMBER=    115601  CLASS NUMBER=     45
IDEAL CLASSES
( 1, 0+M)
( 166, 13+M)
( 173, 13+M)
( 155, 19+M)
( 184, 19+M)
( 160, 20+M)
( 178, 20+M)
( 163, 34+M)
( 170, 34+M)
( 145, 40+M)
( 188, 40+M)
( 128, 43+M)
( 211, 43+M)
( 155, 50+M)
( 170, 50+M)
( 136, 51+M)
( 193, 51+M)
( 152, 52+M)
( 172, 52+M)
( 134, 57+M)
( 191, 57+M)
( 107, 65+M)
( 230, 65+M)
( 115, 65+M)
( 214, 65+M)
( 136, 67+M)
( 179, 67+M)
( 100, 75+M)
( 232, 75+M)
( 118, 80+M)
( 190, 80+M)
( 85, 0+M)
( 254, 85+M)
( 94, 87+M)
( 226, 87+M)
( 92, 88+M)
( 229, 88+M)
( 86, 9+M)
( 230, 95+M)
( 50, 24+M)
( 268, 124+M)
( 34, 0+M)
( 302, 136+M)
( 17, 0+M)
( 314, 153+M)

```

計算例

うしなくてもよいのである。その代り S の元が発生するごとにその展開をする必要がある。しかしこのため記憶番地は、類数の数以上であればよいのだから随分の節約である。

a は $(1), (1')$ の条件で、 $(m-b^2)/4$ または $m-b^2$ (これらを以下 d とおく) の因数から選出するのであるが、手数をはぶくため、選出は $[\sqrt{d}]$ までにして残りは補因数として扱うようにした。 $a=1$ の場合は主類になるから選出しなくてもよい。しかし補因数 $a=d$ の場合は考慮がいる。——この考慮は、 $[(\sqrt{m}-b)/2]+1$ または $[\sqrt{m}]-b+1$ が1となると必要であるが、因数選出で1は出さないようにしたので特別

に扱うようにした。——プログラム第29行, 第30行と第48行, 第49行。

主な変数との対応, M: m , MS: $[\sqrt{m}]$, C2: b , CLN: 類数

FACTOR, SELECT, PRSB および KETT はそれぞれ因数分解, 因数の選出, 素数の発生, および展開のサブルーチンである。なお FACTOR, SELECT は筆者のプログラム^{1), 4)}の MAIN からの分離である。

代表イデアルは各 S_0 の元から $m \equiv 1, m \not\equiv 1 \pmod{4}$ に従ってそれぞれ

$$\left[a, \frac{b-1}{2} + w \right] \quad \text{ただし } w = \frac{1 + \sqrt{m}}{2},$$

$$[a, b + w] \quad \text{ただし } w = \sqrt{m}$$

$(b-1)/2, b$ は $\pmod{a}$ で表示する。配列 U2, V2 は展開の終項用; U, V はイデアル用である。

小型計算機の場合には U2, V2 だけにするとか、配列 B の素数をディスクに記憶させるなどで、更に番地の節約をする。

2. テスト結果

計算機は FACOM M-190 (京都大学) を使用した。次はその結果で, TOTAL CPU TIME 4 SEC である。

なお, サブルーチン SQFREE⁴⁾ を用いて, $m=2$ から $m=681$ までの 2 次体について, 類数と代表イデアルが直に出力 (プリント) された。

参 考 文 献

- 1) 片山: 実 2 次数体の類数の計算, 情報処理, Vol. 16, No. 9, pp. 822~824 (1975).
- 2) 片山: 2 次数体のイデアル類群の計算, 情報処理掲載予定.
- 3) 高木: 初等整数論講義, 共立出版 (1971).
- 4) 片山: 虚 2 次数体の類数の計算, 情報処理, Vol. 18, No. 6, pp. 612~613 (1977).

(昭和 52 年 9 月 2 日受付)