プログラムのページ

77-03 虚2次数体の類数の計算

片山　茂*

虚2次数体の類数とその類の代表イデアルを求めるプログラムについて述べる.

1. 計算法

mを素数の平方では割れない自然数とする. このとき

$$d=\begin{cases} m, & m\equiv 3 \pmod 4 \text{ のとき}, \\ 4m, & m\not\equiv 3 \pmod 4 \text{ のとき} \end{cases}$$

ときめる. $(-d)$ を判別式にもつ虚2次数体の類数とは

(1)　$|b_1|\leqq a\leqq c$,

($|b_1|=a$ のとき $b_1>0$, $a=c$ のとき $b_1\geqq 0$),

(2)　$|b_1|\leqq\sqrt{\dfrac{d}{3}}$,

(3)　$ac=(d+b_1^2)/4$

をみたす a, b_1, c の組み合わせの個数のことで, また組の代表イデアルは

$d=4m$, m に従ってそれぞれ

$[a, -b_1/2+\mathrm{w}]$** (ただし $\mathrm{w}=\sqrt{-m}$),

$[a, (-b_1-1)/2+\mathrm{w}]$** $\left(\text{ただし } \mathrm{w}=\dfrac{1+\sqrt{-m}}{2}\right)$

である[1].

a, b_1, c の組を求める手順は, まず d, m の定め方から $m\equiv 3 \pmod 4$, $m\not\equiv 3 \pmod 4$ に従って $|b_1|$ はそれぞれ奇数, 偶数をとることに注意して, b $(\geqq 0)$ を $b\leqq\sqrt{d/3}$ できめて, $d_1=(d+b^2)/4$ とおく.

第1段, $d_1=1$ となるのは $b=0$, または $b=1$ のときであるから, $a=1, c=d_1$, 類数1, 代表イデアル $[1, \mathrm{w}]$** で終了.

第2段. $d_1\neq 1$ のとき, d_1 を素因数分解して,

$$b\leqq a\leqq[\sqrt{d_1}]^{***}$$

なる d_1 の因数 a を順序づけて求め, $c=d_1/a$ をきめる. ここで $a=b$, または $a=c$, または $b=0$ でないときはもう1組 $-b$ の場合の組を加える. このことを b を $[\sqrt{d/3}]$*** 以下の範囲で2ずつ増加させて繰り返す.

2. プログラム

変数との対応は m : M, d : MD, d_1 : ID, b : IC2, a : AA, c : CC である, CLN は類数である. subroutine PRSB は素数を生成し配列 B に記憶させる[2], subroutine SQFREE は素数の平方で割れない自然数を生成 (または判定) するものである. d_1 の素因数分解, 因数の選出の部分は筆者の実2次数体の類数の計算[3] と同様である.

3. テスト結果

計算例は M=0 とし, SQFREE で1から100までの間の素数の平方で割れない自然数を選出し計算したとき, 虚2次数体 $\boldsymbol{Q}(\sqrt{-95})$, $\boldsymbol{Q}(\sqrt{-97})$ の類数と代表イデアルである (他は略). 適当な変更によって任意の m について判定し, また計算できる.

4. 注　意

筆者の実2次数体の類数の計算のプログラム[3] の一部にその後の使用で誤があり, 本稿のプログラムと関連しているので訂正でせていただく. それは MAIN PROGRAM, 第13行

```
MDS=SQRT(FLOAT(MD))+0.1
```

の +0.1 は不要で誤, 例えば MD=32009 とすると, 必要なのは $[\sqrt{32009}]$*** であるから. 第53行についても同様である.

このことから本稿のプログラム (MAIN) 第15行, 第49行はこの注意によった.

参考文献

1) 高木: 初等整数論講義, 共立出版 (1971).
2) 片山: 素数の計算, 情報処理, Vol. 15, No. 11, pp. 903～904 (1974).
3) ——: 実2次数体の類数の計算, 情報処理, Vol. 16. No. 9, pp. 822～824 (1975).

(昭和51年8月26日受付)

* 鳥取大学教育学部数学教室

** [,] はイデアルの標準的底表示.

*** [ ] は Gauss の記号.

```
      C   COMPUTATION OF CLASS NUMBER
      C   OF IMAGINARY QUADRATIC NUMBER FIELD
      C   MAIN PROGRAM
    1       INTEGER P(100),E(100),F(100),G(100),
           1B(1252),U(200),V(200)
    2       IMPLICIT INTEGER(A-V)
    3       COMMON B,M
    4       CALL PRSB
    5       M=0
    6   10  CALL SQFREE
    7       IF(MOD(M,4).EQ.3) GO TO 400
    8       MD=4*M
    9       KIGUZ=2
   10       IC2=0
   11       GO TO 401
   12   400 MD=M
   13       KIGUZ=1
   14       IC2=1
   15   401 MD3S=SQRT(FLOAT(MD)/3.0)
   16       N=0
   17   402 ID=(MD+IC2*IC2)/4
   18       IDZ=ID
   19       IF(N.NE.0) GO TO 404
   20       N=N+1
   21       U(N)=1
   22       V(N)=0
   23       IF(ID.EQ.1) GO TO 700
      C   FACTORIZATION OF IDZ
   24   404 I=1
   25       J=0
   26       DO 30 NNN=1,100
   27   30  E(NNN)=0
   28   1   NN=1
   29       BB=B(I)
   30   2   Q=IDZ/BB
   31       IF(IDZ-Q*BB.NE.0) GO TO 4
   32       IF(NN.NE.1) GO TO 3
   33       J=J+1
   34       IF(J.GE.100) STOP 777
   35       P(J)=BB
   36   3   E(J)=E(J)+1
   37       IF(Q.EQ.1) GO TO 6
   38       NN=NN+1
   39       IDZ=Q
   40       GO TO 2
   41   4   IF(Q.LE.BB) GO TO 5
   42       I=I+1
   43       GO TO 1
   44   5   J=J+1
   45       IF(J.GE.100) STOP 7777
   46       P(J)=IDZ
   47       E(J)=E(J)+1
   48   6   JZ=J
      C   SELECTION OF FACTORS
   49       IDS=SQRT(FLOAT(ID))
   50       AA=1
   51       L=1
   52   11  F(L)=0
   53   22  G(L)=AA
   54       L=L+1
   55       IF(L.LE.JZ) GO TO 11
   56       L=JZ
   57   12  F(L)=F(L)+1
   58       IF(F(L).LE.E(L)) GO TO 14
   59   13  L=L-1
   60       IF(L.EQ.0) GO TO 30
   61       AA=G(L)
   62       GO TO 12
   63   14  AA=AA*P(L)
   64       IF(AA.GT.IDS) GO TO 13
   65       IF(AA.LT.IC2) GO TO 22
   66       CC=ID/AA
   67       IF(AA.EQ.IC2.OR.AA.EQ.CC.OR.
           1IC2.EQ.0) GO TO 500
   68       IF(KIGUZ.EQ.2) GO TO 1000
   69       N=N+1
   70   *   U(N)=AA
   71       V(N)=(-IC2)/2
   72       N=N+1
   73       U(N)=AA
   74       V(N)=IC2/2
   75       GO TO 22
   76   1000 N=N+1
   77       U(N)=AA
   78       V(N)=(-IC2-1)/2
   79       N=N+1
   80       U(N)=AA
   81       V(N)=(IC2-1)/2
   82       GO TO 22
   83   500 IF(KIGUZ.EQ.1) GO TO 1001
   84       N=N+1
   85       U(N)=AA
   86       V(N)=(-IC2)/2
   87       GO TO 22
   88   1001 N=N+1
   89       U(N)=AA
   90       V(N)=(-IC2-1)/2
   91       GO TO 22
   92   50  IC2=IC2+2
   93       IF(IC2.LE.MD3S) GO TO 402
   94   700 IM=-M
   95       CLN=N
   96       WRITE(6,201) IM,CLN
   97   201 FORMAT(1H0,7X,7HNUMBER=,I3,
           12X,13HCLASS NUMBER=,I3)
   98       WRITE(6,202)
   99   202 FORMAT(1H ,7X,13HIDEAL CLASSES)
  100       WRITE(6,203) (U(J),V(J),J=1,CLN)
  101   203 FORMAT(1H ,20X,1H(,I2,1H+,I3,3H*W))
  102       GO TO 10
  103       END
```

```
    1       SUBROUTINE SQFREE
    2       INTEGER B(1252),BB,Q
    3       COMMON B,M
    4   1   I=1
    5       M=M+1
    6       IF(M.GT.100) STOP
    7       MM=M
    8   2   NN=1
    9       BB=B(I)
   10   3   Q=MM/BB
   11       IF(MM-Q*BB.NE.0) GO TO 4
   12       IF(NN.NE.1) GO TO 1
   13       IF(Q.EQ.1) GO TO 20
   14       NN=NN+1
   15       MM=Q
   16       GO TO 3
   17   4   IF(Q.LE.BB) GO TO 20
   18       I=I+1
   19       GO TO 2
   20   20  RETURN
   21       END
```

```
 NUMBER=-95  CLASS NUMBER=  8
 IDEAL CLASSES
                ( 1,  0+W)
                ( 3, -1+W)
                ( 3,  0+W)
                ( 2, -1+W)
                ( 2,  0+W)
                ( 4, -1+W)
                ( 4,  0+W)
                ( 5, -3+W)

 NUMBER=-97  CLASS NUMBER=  4
 IDEAL CLASSES
                ( 1,  0+W)
                ( 7, -1+W)
                ( 7,  1+W)
                ( 2, -1+W)
```

計 算 例