円分多項式（Cyclotomic Polynomial）の係数の計算

ライブラリー・プログラム研究
開発計画成果報告(利用手引書)

鹿児島大学　教養部数学科
小　柴　洋　一

はじめに，入力と出力を明記しておきます．

入力：円分多項式の次数（注意：単なる多項式としての次数ではない）
　　1個の整数型のデータ
　　バッチの場合は更に文字列 'ＹＥＳ' 又は 'ＮＯ' を3個入力．

出力：その時の円分多項式の係数
　　各次数の係数が整数型のデータとして出力される．

§1．プログラムの目的　利用可能な計算機は　ＳＸ（バッチ）及びＡＣＯＳ（ＴＳＳ）．適用分野，用途は　数学・整数論．
想定されるユーザーは，数学計算の情報結果に関心のある方全て．
形態は，独立のプログラムの形をとっています．言語は FORTRAN.
このプログラムは，大阪大学大型計算機センターの研究開発課題として認められたものです．

§2．背景・理論　円分多項式は，代数的整数論において円分体の定義方程式であります．円分多項式とは，何か，という定義は，標準的な書物をみていただくことにします（van der Waerden［1］）．この多項式を紙とエンピツで計算してみると次数が低いときはその係数が−1，0，1のみに限られるような直感をもつ．この直感が正しくない事が次数が105のときの計算から解る．この105計算でも手計算にしては大変な計算量である.アメリカの LEHMER が1930年代に，種々計算したことが伝えられている．
この計算は，本来の定義からして必然的に高速計算と広い領域を必要とします．
パソコンやワークステーション上で数式処理ソフトウエアを用いて行なう例もあるが（森本［3］）が，数式処理ソフトを用いた手法では，高次の円分多項式の係数の決定に必要な計算時間が膨大なものとなる．そこで本プログラムは，スーパコン上のＦＯＲＴＲＡＮによつて，数式処理によるものより，はるかに高速に高次の円分多項式の係数を与えることを目的として開発したものである．

§３．本プログラムの利用方法

ＴＳＳ処理の場合：

ＳＹＳＴＥＭ　モードで次のように入力する（次数105の場合）．

SYSTEM？ CRUN LIBSOURCE/APPLIC/CYCPLY/CYCTSS；；（105）

（　　）の中に105を与えたがこの値は　４００００までの自然数であればＴＳＳセッション中に答を端末に出力する．

バツチ処理の場合：

ＪＯＢ制御文の例をあげておく．

```
００１０$        JOB          ；A，V
００２０$        SX           CPTIME＝10800
００３０$        FRT77        VECTOR＝(LOOPCNT＝5000000)
００４０$        SELECTA      LIBSOURCE / APPLIC / CYCPLY / CYCSX
００５０$        GO
００７０         210
００８０ＹＥＳ
００９０ＹＥＳ
０１００ＹＥＳ
０１１０$        PRMFL        16，W，S，A＃＃＃＃＃ / FILE16
０１２０$        PRMFL        17，W，S，A＃＃＃＃＃ / FILE17
０１３０$        PRMFL        18，W，S，A＃＃＃＃＃ / FILE18
０１４０$        ENDJOB
```

上の文で　Ａ＃＃＃＃＃ は　利用者番号である．

ＲＥＡＤ文が４個あり，４個の入力データを順に説明する．

第１入力データ：整数型データ．

円分多項式の次数．０＜Ｎ＜５０００００００　なる整数Ｎ．

この範囲以外の整数を与えると実行は止まる．

第２入力データ：文字列’ＹＥＳ’又は’ＮＯ’

文字列’ＹＥＳ’を入力すると，円分多項式が降べきの順に出力される．

この出力が必要ないときは’ＮＯ’

文字列’ＹＥＳ’または’ＮＯ’以外のときは，実行は止まる．

第３入力データ：文字列’ＹＥＳ’または’ＮＯ’

文字列’ＹＥＳ’を入力すると，係数の値を同じものをまとめて，大きいものから順に出力される．

この出力が必要ないときは’ＮＯ’．

文字列 ' ＹＥＳ ' 又は ' ＮＯ ' 以外のときは，実行は止まる．

第４入力データ：文字列 ' ＹＥＳ ' 又は ' ＮＯ '

文字列 ' ＹＥＳ ' を入力すると，係数の値の頻度を出力される．

この出力が必要ないときは ' ＮＯ '．

文字列 ' ＹＥＳ ' 又は ' ＮＯ ' 以外のときは，実行は止まる．

§４．入力パラメーター

第１入力データの値が大きいときは，実行時間が長くかかる（たとえば 2883737 次では cputime は約 700 秒であった）ので注意が必要.第2～第4入力データで文字列 ' ＹＥＳ ' を与えた場合，ソースプログラムの中でこの順で WRITE（16, ……），WRITE（17, ……），WRITE（18, ……）になっているのでファイル出力として機番16, 17, 18に対応するＪＯＢ制御文を与えねばならない．なお，第１入力データの値が大きいときには，このファイル出力も大きくなる（2883737 次に対して16が約５万LLINK, 17が３万LLINK 程度）ことにも注意が必要である．

ソースプログラム（FORTRAN）の中で配列宣言の前に PARAMETER 文がある．プログラムの大体の大きさはこの PARAMETER 文で与えた値の４倍の整数データが必要で，これが機械語の大部分を占めている．ソースプログラムが公開されているので各自の ファイルに コピー してきて PARAMETER 文の値をＪＯＢクラスに応じて変えると良い．

§５．出力リストの見方

ＴＳＳ処理の場合：

昇巾の順に　degree.＝value の形で出る．

実行例でみてください．

バツチ出力の場合：

機番16については　前半部分には約数（divisor）と Euler 関数の値（Euler number）が出る．後半部分は　ＴＳＳ処理の場合と同じ．

機番17については　同じ係数値をもつ次数をまとめている．

機番18については　機番17の次数項の個数を表わしている．

§６．実行例

ＴＳＳ処理の場合：

SYSTEM? CRUN LIBSOURCE / APPLIC / CYCPLY / CYCTSS ; ; (105)

```
*******************************************************************************
*                                                                             *
*               THE   COMPUTATIONS OF      105-TH CYCLOTOMIC  POLYNOMIAL:     *
*                                                                             *
*******************************************************************************
        0.=      1:        1.=      1:        2.=      1:        3.=      0
        4.=      0:        5.=     -1:        6.=     -1:        7.=     -2
        8.=     -1:        9.=     -1:       10.=      0:       11.=      0
       12.=      1:       13.=      1:       14.=      1:       15.=      1
       16.=      1:       17.=      1:       18.=      0:       19.=      0
       20.=     -1:       21.=      0:       22.=     -1:       23.=      0
       24.=     -1:       25.=      0:       26.=     -1:       27.=      0
       28.=     -1:       29.=      0:       30.=      0:       31.=      1
       32.=      1:       33.=      1:       34.=      1:       35.=      1
       36.=      1:       37.=      0:       38.=      0:       39.=     -1
       40.=     -1:       41.=     -2:       42.=     -1:       43.=     -1
       44.=      0:       45.=      0:       46.=      1:       47.=      1
       48.=      1
```

上の出力を普通の数学の書式で述べると

$$\chi^{48}+\chi^{47}+\chi^{46}+\chi^{43}+\chi^{42}-2\chi^{41}-\chi^{40}-\chi^{39}+\chi^{36}+\chi^{35}+\chi^{34}+\chi^{33}+\chi^{32}+\chi^{31}-\chi^{28}-\chi^{26}-\chi^{24}-\chi^{22}-$$

$$\chi^{20}+\chi^{17}+\chi^{16}+\chi^{15}+\chi^{14}+\chi^{13}+\chi^{12}-\chi^{9}-\chi^{8}-2\chi^{7}-\chi^{6}-\chi^{5}+\chi^{2}+\chi+1$$

という形の多項式が　105-th の円分多項式として計算されたことになる.

バッチ処理の場合：

SYSTEM ?

LIST FILE16

```
*******************************************************************************
*                                                                             *
*               THE   COMPUTATIONS OF      210-TH CYCLOTOMIC  POLYNOMIAL:     *
*                                                                             *
*******************************************************************************

JJJ=226N123=210ZAHL=16
 ORDER=    2    DIVISOR=        2    EULER NUMBER=       1
 ORDER=    3    DIVISOR=        3    EULER NUMBER=       2
 ORDER=    4    DIVISOR=        5    EULER NUMBER=       4
 ORDER=    5    DIVISOR=        6    EULER NUMBER=       2
 ORDER=    6    DIVISOR=        7    EULER NUMBER=       6
 ORDER=    7    DIVISOR=       10    EULER NUMBER=       4
 ORDER=    8    DIVISOR=       14    EULER NUMBER=       6
 ORDER=    9    DIVISOR=       15    EULER NUMBER=       8
 ORDER=   10    DIVISOR=       21    EULER NUMBER=      12
 ORDER=   11    DIVISOR=       30    EULER NUMBER=       8
 ORDER=   12    DIVISOR=       35    EULER NUMBER=      24
 ORDER=   13    DIVISOR=       42    EULER NUMBER=      12
 ORDER=   14    DIVISOR=       70    EULER NUMBER=      24
 ORDER=   15    DIVISOR=      105    EULER NUMBER=      48
```

```
 ORDER=  16   DIVISOR=     210   EULER NUMBER=     48
KKK=225
         0.=      1:        1.=     -1:        2.=      1:        3.=      0
         4.=      0:        5.=      1:        6.=     -1:        7.=      2
         8.=     -1:        9.=      1:       10.=      0:       11.=      0
        12.=      1:       13.=     -1:       14.=      1:       15.=     -1
        16.=      1:       17.=     -1:       18.=      0:       19.=      0
        20.=     -1:       21.=      0:       22.=     -1:       23.=      0
        24.=     -1:       25.=      0:       26.=     -1:       27.=      0
        28.=     -1:       29.=      0:       30.=      0:       31.=     -1
        32.=      1:       33.=     -1:       34.=      1:       35.=     -1
        36.=      1:       37.=      0:       38.=      0:       39.=      1
        40.=     -1:       41.=      2:       42.=     -1:       43.=      1
        44.=      0:       45.=      0:       46.=      1:       47.=     -1
        48.=      1

SYSTEM ?
LIST FILE17

*****************************************************************************
*                                                                           *
*     THE DISTRIBUTIONS OF THE VALUE OF COEFFICIENTS       210-TH           *
*                                                                           *
*****************************************************************************


 COEFFICIENT=     -1:
         1,         6,         8,        13,        15,        17,        20,
        22,        24,        26,        28,        31,        33,        35,
        40,        42,        47
NUMBER OF COEF.=17


 COEFFICIENT=      0:
         3,         4,        10,        11,        18,        19,        21,
        23,        25,        27,        29,        30,        37,        38,
        44,        45
NUMBER OF COEF.=16


 COEFFICIENT=      1:
         0,         2,         5,         9,        12,        14,        16,
        32,        34,        36,        39,        43,        46,        48
NUMBER OF COEF.=14


 COEFFICIENT=      2:
         7,        41

NUMBER OF COEF.=2
```

```
SYSTEM ?
LIST FILE18

THE HISTOGRAMME OF THE VALUE OF THE COEFFICIENTS :210-TH
 NUMBER    OF TERMS WITH VALUE     -1=      17 :
 NUMBER    OF TERMS WITH VALUE      0=      16 :
 NUMBER    OF TERMS WITH VALUE      1=      14 :
 NUMBER    OF TERMS WITH VALUE      2=       2 :
```

参考文献：

1．van der Waerden（ファン・デル・ヴェルデン），現代代数学　1，銀林訳，東京図書，148ページ．

2．高木貞治，初等整数論講義，共立出版．

3．森本光生，muMATH で学ぶ整数論，数学セミナー，vol. 25 no. 5～vol. 26 no. 4