円分多項式(Cyclotomic Polynomial)の係数の計算

小柴, 洋一
鹿児島大学理学部数理情報科学科

https://doi.org/10.15017/1470308

出版情報：九州大学大型計算機センター広報. 30 (2), pp.141-145, 1997-06. 九州大学大型計算機センター
バージョン：
権利関係：

円分多項式 (Cyclotomic Polynomial) の係数の計算

小柴 洋一 *

プログラムライブラリ開発計画に表記の課題で参加させていただいたのでその報告も兼ねて寄稿します.

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 4 バイト整数型 (以下単に整数型) のデータ
	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 このプログラムは何を計算するのか

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と (van der Waerden[1]) そこに書いてありますが，末尾に簡単な定義，公式を述べておきました．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ってしまいがちです．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ります．この 105 の計算でも手計算にしては大変な計算量です．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ます.

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ります (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ります．ソフトウエア *Mathematica* で装備されている函数 Cyclotomic も同じ計算を行ないますが小規模のものにならざるをえません.

そこで本プログラムは，スーパーコンピュータ上の FORTRAN によって，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す.

2 本プログラムの利用方法

READ 文が 4 個あり，4 個の入力データを順に説明します.

第 1 入力データ：	整数型データ.
	円分多項式の次数. 0<N<5000000 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' 又は 'NO' 以外のときは，実行は止まる.

*鹿児島大理学部数理情報科学科　E-mail : koshiba@cla.kagoshima-u.ac.jp

第3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せる.
	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.

3 入力パラメーター

メモリー量について：ソースプログラム (FORTRAN) の中で配列宣言の前に PARAMETER 文があります．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ます．ソースプログラムが公開されているので各自のデータセットにコピーしてきて PARAMETER 文の値を JOB クラスに応じて変えて下さい．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ので注意が必要です．第2, 第3, 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 $WRITE(16,\cdots), WRITE(17,\cdots), WRITE(18,\cdots)$ になっているのでデータセット出力として機番 16, 17, 18 に対応する JOB 制御文を与えねばなりません (または UXP 上ではそれに類するシェルスクリプトを書かねばなりません).

4 出力リストの見方

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) が出ます．機番17については，同じ係数値をもつ次数をまとめています．機番18については，機番17の次数項の個数を表わしています.

5 実行例

MSP の下で機番16に割り当てられたデータセット DATA1 の内容をみます.

```
 READY
LIST DATA1

*****************************************************************************
*                                                                           *
*              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

$$\Phi_{105}(x) = 1 + x + x^2 - x^5 - x^6 - 2x^7 - x^8 - x^9 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17} - x^{20} - x^{22} - x^{24} - x^{26} - x^{28} + x^{31} + x^{32} + x^{33} + x^{34} + x^{35} + x^{36} - x^{39} - x^{40} - 2x^{41} - x^{42} - x^{43} + x^{46} + x^{47} + x^{48}$$

という形の変数 x の多項式が 105-th の円分多項式 $\Phi_{105}(x)$ として計算されたことになります.

バッチ処理の場合：

後で制御文の例を出しますが、そこで実行生成された出力ファイルの内容の例は以下の通りです.

```
 READY
LIST CYC16.DATA

*****************************************************************************
*                                                                           *
*               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
```

同様に CYC17.DATA をみると

```
 READY
LIST CYC17.DATA

*****************************************************************************
*                                                                           *
*     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
```

同様に CYC18.DATA をみると

```
 READY
LIST CYC18.DATA

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 :
```

JOB 制御文の例をあげておきます.

```
//A71234BA JOB PASSWORD,CLASS=Y,TIME=(1430,0),NOTIFY=A71234
// EXEC FORT,VPP=YES
//FORT.SYSIN DD DSN=CYC.FORT,DISP=SHR
//GO.SYSIN DD *
255255
YES
YES
YES
/*
//GO.FT16F001 DD DSN=CYC16.DATA,DISP=(NEW,CATLG),SPACE=(CYL,(10,1))
//GO.FT17F001 DD DSN=CYC17.DATA,DISP=(NEW,CATLG),SPACE=(CYL,(10,1)),
//     DCB=(RECFM=FB,LRECL=133,BLKSIZE=3120)
//GO.FT18F001 DD DSN=CYC18.DATA,DISP=(NEW,CATLG),SPACE=(TRK,(10,5))
//
```

$255255 = 3\times5\times7\times11\times13\times17$ の円分多項式を計算してデータセット CYC16.DATA, CYC17.DATA, CYC18.DATA に機番 16, 17, 18 に応じて出力しています.

上の説明から解るように UXP でのバッチジョブも殆ど同じです. 一応書いておくと入力データファイルとして例えばファイル cyc.dat をエディタで以下のように作ります.

```
105
YES
YES
YES
```

バッチのシェルスクリプトを例えばファイル cyc.sh として以下のようにエディタで作ります.

```
setenv fu16 fort16
setenv fu17 fort17
setenv fu18 fort18
frt cyc.f
a.out < cyc.dat
```

ファイル cyc.f は円分多項式を計算する肝心要の FORTRAN プログラムファイルです．ソースプログラムは kyu-cc の /usr/local/doc/cyc.f として公開します．各自以下の要領でコピーできます．

```
cp /usr/local/doc/cyc.f .
```

これをバッチファイルとします．

```
qsub -q p1 cyc.sh
```

円分多項式の 定義
多項式 x^n-1 の解を複素数の範囲で考えます． n 個の根のなかで原始的なものを全部とってきて $\zeta_1,\cdots,\zeta_m$ とします．次の多項式

$$\Phi_n(x)=(x-\zeta_1)\cdots(x-\zeta_m)$$

を $n-th$ 円分多項式といいます．
この式は一見　複素数のままの係数のようにみえますが、展開するとその係数は整数になります．有理数体上既約であることが知られています．

公式

$$x^n-1=\prod_{d|n}\Phi_d(x)$$

があり右辺は左辺の因数分解を与えていることになりますが本プログラムのアルゴリズムはこの公式に依っています．

参考文献

[1] van der Waerden(ファン・デル・ヴェルデン), 現代代数学 第1巻, 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． 61 ページ.

[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.

[4] 小柴洋一, 円分多項式の係数の計算 大阪大学大型計算機センターニュース　Vol.21, No.2, 1991-8, 82, pp.51-56.