# 2 次の DBPS(2 重基底多項式篩法)による因数分解例

2006/5/25 後 保範
2006/5/30 改 定

1. 概要

合成数 $N$ に対して 2 次関数 $f(x)$ を使用して篩を行い、因数分解する。

$f(x) = Ax^2 + Bx + C,\ f(M) \equiv 0 \pmod{N}$ に対して下記の様に関数 $g(x)$ を定義する。

$$g(x) = (cAx + a)(dx + b) - cdf(x) = sx + t$$
$$s = ad + c(bA - dB),\ t = ab - cdC$$

すると、関数 $f(x)$ と数値 $N$ に対する剰余が下記で与えられる。

$$g(x) = (cAx + a)(dx + b) \equiv sx + t \pmod{f(x)} \quad \text{--- (1)}$$
$$(cAM + a)(dM + b) = sM + t \pmod{N} \quad \text{--- (2)}$$

(2)式に素数と一次式の 2 つの基底を使用して篩をおこなう。

即ち、素数基底と一次式基底を使用して、$cAM + a, dM + b$ 及び $sM + t$ を篩により分解する。素数基底は-1 と小さい素数より順に選ぶ。一次式基底は素数基底で分解できない $\alpha M + \beta$ に対して、$\alpha, \beta$ が小さい整数で出現頻度が多いもの順に選ぶ。

本方式を MBPS(Multiple Base Polynomial Sieve、多重基底多項式篩法)の一種の DBPS(Double Base Polynomial Sieve、2 重基底多項式篩法)と名付ける。

DBPS は MPQS(複数多項式 2 次篩法)と同様に、多数の関数 $f(x)$ を使用できる。

2. 計算対象

$N = 55751$ を DBPS で因数分解する。

篩には下記の多項式 $f(x)$ を使用する。説明を簡単にするため 1 個の関数だけ使用する。

$$f(x) = 2x^2 - 27,\ f(M) = N,\ M = 167$$

素数基底は-1 と 2,3,5,7,11,13,17,19,23 の 9 個の素数を使用する。

一次式基底は M-3,M,2M+1,2M+3 及び 2M+5 の 5 個を使用する。

3. 素数及び一次式による篩

$c = 1, d = 1$ かつ、$a, b, s$ の絶対値が 9 以下のもので篩を行う。素数と一次式の基底の合計は 15 個となるので、篩の結果はそれより 7 個多く 22 個を選定した。

表 1 に篩結果の行列を示す。表 1 中の一次式基底の B1,B2,B3,B4 及び B5 はそれぞれ M-3,M,2M+1,2M+3 及び 2M+5 に対応する。表 1 の正のベキは左辺での指数を、負のベキは右辺での指数を示す。従って、表 1 の No.1～No.4 は(mod N)の基で下記の等式を示す。No.5 以下も同様である。

No.1 : $2M(M+3) \equiv 3(2M+9) \rightarrow 2^2 \cdot 5 \cdot 17 \cdot M \equiv 3 \cdot 7^3$

No.2 : $2M(M+1) \equiv 2M+27 \rightarrow 2^4 \cdot 3 \cdot 7 \cdot M \equiv 19^2$

No.3 : $2M^2 \equiv 27 \rightarrow 2 \cdot M^2 \equiv 3^3$

No.4 : $2M(M-3) \equiv -3(2M-9) \rightarrow 2 \cdot (M-3) \cdot M \equiv -1 \cdot 3 \cdot 5^2 \cdot 13$

表 1.　2 次の DBPS による篩結果の行列 (c,d=1)

| No | g(x)の係数 | | mod N での等式 | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 素数基底 | | | | | | | | | | 一次式基底 | | | | |
| | a | b | -1 | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | B1 | B2 | B3 | B4 | B5 |
| 1 | 0 | 3 | 0 | 2 | -1 | 1 | -3 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 2 | 0 | 1 | 0 | 4 | 1 | 0 | 1 | 0 | 0 | 0 | -2 | 0 | 0 | 1 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 1 | -3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| 4 | 0 | -3 | 1 | 1 | -1 | -2 | 0 | 0 | -1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 5 | 1 | 2 | 0 | -5 | -3 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 6 | 1 | 1 | 0 | 3 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | -2 | 0 | 0 | 1 | 0 | 0 |
| 7 | 1 | -2 | 1 | -2 | 1 | 1 | -1 | 1 | 0 | -1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 8 | 3 | 3 | 0 | 1 | -4 | 1 | 0 | 0 | 0 | 1 | -1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 9 | 3 | 0 | 0 | -4 | -1 | 0 | 0 | -1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 10 | 3 | -3 | 1 | 0 | -1 | 0 | -1 | 0 | 0 | 0 | 0 | -1 | 1 | 0 | 0 | 1 | 0 |
| 11 | 4 | -2 | 0 | 1 | 1 | 1 | 0 | 1 | 2 | 0 | -1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 5 | 2 | 0 | -2 | 0 | -1 | -1 | -1 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 13 | 5 | -2 | 0 | -3 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | -1 | 0 | 0 | 0 | 0 | 1 |
| 14 | 5 | -5 | 1 | 1 | 4 | 0 | -2 | 0 | 0 | -1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 15 | 6 | -3 | 0 | 2 | -2 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 16 | 6 | -6 | 1 | 2 | -1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | -1 | 0 |
| 17 | 9 | 0 | 0 | -1 | -2 | -1 | 3 | 0 | 0 | -1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 18 | 9 | -3 | 0 | 0 | -1 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 1 | -1 | 0 | 0 | 0 |
| 19 | 9 | -6 | 1 | -4 | -1 | 0 | 4 | -1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 20 | -9 | 9 | 0 | 4 | -2 | 2 | -1 | 1 | 1 | 0 | 0 | -1 | 0 | 0 | 0 | 0 | 0 |
| 21 | -9 | 4 | 1 | -4 | 2 | 2 | 0 | -1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 22 | -9 | 3 | 1 | 1 | -1 | 3 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | -1 | 0 | 0 | 0 |

4. 従属行の決定

(1)　従属行計算行列

表 1 に 15 個の基底(素数と一次式)に対応する部分の 2 の剰余から下記の行列(22×16 次元)が作成される。

0 0 1 1 1 0 0 1 0 0 0 1 0 0 0
0 0 1 0 1 0 0 0 0 0 0 1 0 0 0
0 1 1 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 1 0 0 0 1 1 0 0 0
0 1 1 0 0 0 0 0 0 0 0 0 1 0 0
0 1 1 0 1 0 0 0 0 0 0 0 1 0 0
1 0 1 1 1 1 0 1 0 0 0 0 1 0 0
0 1 0 1 0 0 0 1 1 0 0 0 0 1 0
0 0 1 0 0 1 0 0 0 0 0 1 0 1 0

```
    1 0 1 0 1 0 0 0 0 1 1 0 0 1 0
    0 1 1 1 0 1 0 0 1 0 0 0 0 0 0
A = 0 0 0 1 1 1 0 0 0 0 0 0 0 0 1
    0 1 1 1 0 1 0 0 0 1 0 0 0 0 1
    1 1 0 0 0 0 0 1 0 0 0 0 0 0 1
    0 0 0 1 0 0 0 1 0 0 1 0 0 0 0
    1 0 1 1 1 0 0 1 0 1 0 0 0 1 0
    0 0 0 1 0 0 0 1 0 0 1 0 0 0 0
    0 0 1 0 1 0 0 0 0 0 1 1 0 0 0
    1 0 1 0 0 1 0 0 0 1 0 0 0 0 0
    0 0 0 0 1 1 1 0 0 1 0 0 0 0 0
    1 0 0 0 0 1 1 0 1 0 0 0 0 0 0
    1 1 1 1 0 0 1 1 0 0 0 1 0 0 0
```

(2) 行列消去

単位行列をEとする、行列Aの右にEを追加して行列AをEと合わせて消去する。

行列Aの下三角部分が総てゼロとなるEの消去結果を下記に示す。

この最後の 9 行が従属となる行列の行番号を示す。

```
                        消去後のE
行   |  0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 2 2 2 <-- 列番号(10)
番号 |  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 <-- 列番号(1)
-----------------------------------------------------------------
14   |  0 0 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0
15   |  0 1 0 0 1 0 1 0 1 1 0 1 1 0 1 0 0 0 0 0 0 0
16   |  0 1 0 0 1 0 1 0 1 0 0 1 1 0 0 1 0 0 0 0 0 0
17   |  0 1 0 0 1 0 1 0 1 1 0 1 1 0 0 0 1 0 0 0 0 0
18   |  1 1 0 0 1 0 1 0 1 1 0 1 1 0 0 0 0 1 0 0 0 0
19   |  1 1 0 0 1 0 1 0 0 0 0 1 1 0 0 0 0 0 1 0 0 0
20   |  0 0 1 1 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 1 0 0
21   |  0 1 0 1 1 0 1 1 0 1 0 1 1 0 0 0 0 0 0 0 1 0
22   |  0 1 0 1 1 0 1 0 1 1 0 1 1 0 0 0 0 0 0 0 0 1
```

(3) 従属行

行列消去し、行列Aが全てゼロになった行のEの行で非ゼロとなる列が従属行を示す。

従って、従属行は 9 組あり次のようになる。

(a) 従属行 1 ： 5, 7, 12, 14

(b) 従属行 2 ： 2, 5, 7, 9, 10, 12, 13, 15

(c) 従属行 3 ： 2, 5, 7, 9, 12, 13, 16

(d) 従属行 4 ： 1, 3, 17

(e) 従属行 5 ： 1, 2, 5, 7, 9, 10, 12, 13, 18

(f) 従属行 6 ： 1, 2, 5, 7, 12, 13, 19

(g) 従属行 7 ： 3, 4, 9, 10, 20

(h) 従属行 8 ： 2, 4, 5, 7, 8, 10, 12, 13, 21

(i) 従属行 9 ： 2, 4, 5, 7, 9, 10, 12, 13, 22

5. 因数分解

(1) 従属行 1：15,7,12,14

表 1 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(3\cdot13^2\cdot335\cdot339)^2 \equiv (2^4\cdot7^2\cdot17)^2 \pmod{55751}$

計算すると下記のようになる。

$13328^2 \equiv 13328^2 \pmod{55751}$

これは自明解のため分解できない。

(2) 従属行 2：2,5,7,9,10,12,13,15

表 1 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(5\cdot13^2\cdot164\cdot167\cdot335\cdot337\cdot339)^2 \equiv (2^5\cdot3^2\cdot7\cdot19\cdot23)^2 \pmod{55751}$

計算すると下記のようになる。

$24042^2 \equiv 11024^2 \pmod{55751}$

従って下記のようになる。

GCD(24042-11024,55751)=283, GCD(24042+11024,55751)=197

即ち、55751=197·283 となる。

(3) 従属行 3：2,5,7,9,12,13,16

同様に、下記が成立する。

$11477^2 \equiv 1824^2 \pmod{55751}$

従って、55751=197·283 となる。

(4) 従属行 4：1, 3, 17

同様に、下記が成立する。

$27^2 \equiv 27^2 \pmod{55751}$

これは自明解のため分解できない。

(5) 従属行 5：1,2,5,7,9,10,12,13,18

同様に、下記が成立する。

$24042^2 \equiv 11024^2 \pmod{55751}$

従って、55751=197·283 となる。

(6) 従属行 6：1,2,5,7,12,13,19

同様に、下記が成立する。

$11477^2 \equiv 1824^2 \pmod{55751}$

従って、55751=197·283 となる。

(7) 従属行 7：3,4,9,10,20

同様に、下記が成立する。

$13041^2 \equiv 13041^2 \pmod{55751}$

これは自明解のため分解できない。

(8) 従属行 8：2,4,5,7,8,10,12,13,21

同様に、下記が成立する。

$24042^2 \equiv 11024^2 \pmod{55751}$

従って、55751=197·283 となる。

(9) 従属行 9：2,4,5,7,9,10,12,13,22

同様に、下記が成立する。

$24042^2 \equiv 11024^2 \pmod{55751}$

従って、55751=197·283 となる。