2 次の TBPS2 による因数分解例

2006/08/16　　後 保範

1. 概要

TBPS(3 重基底多項式篩法)を改良した TBPS2(Triple Base Polynomial Sieve 2nd)を使用して因数分解する例を示す。

$f(x)=Ax^2+Bx+C,\ f(M)\equiv 0 \pmod N$ となる、2 次多項式 $f(x)$ と整数 M を求める。このとき、TBPS2 では $A\theta+a$ 及び $\theta+b$ が共に素イデアル基底で分解されるなら、$s\theta+t$ もまた素イデアル基底で分解される性質を利用するのが特長である。

TBPS2 でふるいを行い、ふるいで得られた行列の従属行を算出し、代数平方根を計算して、N を因数分解する。

ふるいの詳細は「2 次の TBPS2 によるふるい例」を参照。

2. 分解対象と使用多項式

N=55751 を素因数分解する。

使用する多項式を下記に示す。

$f(x)=3x^2+2x-9,\ M=136,\ f(M)=N$

3. TBPS2 によるふるい

ふるいの詳細は「2 次の TBPS2 によるふるい例」を参照。

(1) 素数基底と素イデアル基底

素数基底 P は下記のようになり、-1 から 409 を順に P_1 から P_{16} で表す。

P = {-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 67, 137, 409}

素イデアル基底 Q は

Q = {Q_1, Q_2, Q_3, Q_4}とする。

ここで、Q1=(2:1), Q2=(3:1), Q3=(7:2), Q4=(19:5,7)である。

(2) GNFS による基本区間のふるい

イデアル $c\theta+d$ で、$c=1,2,3$ かつ $|d|\le 15$ の範囲でのふるい結果を表 1 に示す。

表 1. 基本区間の GNFS ふるい結果

NO.	イデアル	素数分解		素イデアル分解	
	$c\theta+d$	$cM+d$	P での分解	$N(c\theta+d)$	Q での分解
1	$\theta-3$	133	7･19	24	2^3･3

2	$\theta-2$	134	$2\cdot 67$	7	7
3	$\theta-1$	135	$3^3\cdot 5$	4	2^2
4	θ	136	$2^3\cdot 17$	9	3^2
5	$\theta+1$	137	137	8	2^3
6	$\theta+2$	138	$2\cdot 3\cdot 23$	1	1
7	$\theta+9$	145	$5\cdot 29$	216	$2^3\cdot 3^3$
8	$\theta+12$	148	$3^2\cdot 37$	399	$3\cdot 7\cdot 19$
9	$2\theta+3$	275	$5^2\cdot 11$	21	$3\cdot 7$
10	$3\theta-2$	406	$2\cdot 7\cdot 29$	57	$3\cdot 19$
11	$3\theta-1$	407	$11\cdot 37$	72	$2^3\cdot 3^2$
12	$3\theta+1$	409	409	84	$2^2\cdot 3\cdot 7$
13	$3\theta+2$	410	$2\cdot 5\cdot 41$	81	3^4
14	$3\theta+8$	416	$2^5\cdot 13$	63	$3^2\cdot 7$

(3) DBPS による主ふるい

$Ax+a$ と $x+b$ より下記の式で、s,t を計算する。

$$sx+t=(Ax+a)\cdot(x+b)-f=(Ab+a-B)x+ab-C$$

$$s=Ab+a-B,\quad t=ab-C$$

s,t の最大公約数 G 及び s,t を G で除した S,T を下記で求める。

$$G=sign(s)\cdot GCD(|s|,|t|)$$

$$S=s/G,\quad T=t/G$$

そこで、$1\le S\le 3$ かつ $|T|\le 15$、又は $s=0$ で t が素数基底 P で分解できるものを選ぶ。

表 2 に DBPS による主ふるいを示す。

表 2. DBPS による主ふるい

NO.	入力		出力			採否
	$3x+a$	$x+b$	$sx+t$	G	$Sx+T$	
1	$3(x-1)$	$x-2$	$-11x+15$	−1	$11x-15$	×
2	$3(x-1)$	$x-1$	$-8x+12$	−4	$2x-3$	○
3	$3(x-1)$	x	$-5x+9$	−1	$5x-9$	×
4	$3(x-1)$	$x+1$	$-2x+6$	−2	$x-3$	○
5	$3(x-1)$	$x+2$	$x+3$	1	$x+3$	○
6	$3x-2$	$x-2$	$-10x+13$	−1	$10x-13$	×
7	$3x-2$	$x-1$	$-7x+11$	−1	$7x-11$	×
8	$3x-2$	x	$-4x+9$	−1	$4x-9$	×

9	$3x-2$	$x+1$	$-x+7$	−1	$x-7$	○
10	$3x-2$	$x+2$	$2x+5$	1	$2x+5$	○
11	$3x-1$	$x-2$	$-9x+11$	−1	$9x-11$	×
12	$3x-1$	$x-1$	$-6x+10$	−2	$3x-5$	○
13	$3x-1$	x	$-3x+9$	−3	$x-3$	○
14	$3x-1$	$x+1$	8	1	8	○
15	$3x-1$	$x+2$	$3x+7$	1	$3x+7$	○
16	$3x$	$x-2$	$-8x+9$	−1	$8x-9$	×
17	$3x$	$x-1$	$-5x+9$	−1	$5x-9$	×
18	$3x$	x	$-2x+9$	−1	$2x-9$	○
19	$3x$	$x+1$	$x+9$	1	$x+9$	○
20	$3x$	$x+2$	$4x+9$	1	$4x+9$	×
21	$3x+1$	$x-2$	$-7x+7$	−7	$x-1$	○
22	$3x+1$	$x-1$	$-4x+8$	−2	$2x-4$	○
23	$3x+1$	x	$-x+9$	−1	$x-9$	○
24	$3x+1$	$x+1$	$2x+10$	2	$x+5$	○
25	$3x+1$	$x+2$	$5x+11$	1	$5x+11$	×
26	$3x+2$	$x-2$	$-6x+5$	−1	$6x-5$	×
27	$3x+2$	$x-1$	$-3x+7$	−1	$3x-7$	○
28	$3x+2$	x	9	1	9	○
29	$3x+2$	$x+1$	$3x+11$	1	$3x+11$	○
30	$3x+2$	$x+2$	$6x+13$	1	$6x+13$	×
31	$3(x+1)$	$x-2$	$-5x+3$	−1	$5x-3$	×
32	$3(x+1)$	$x-1$	$-2x+6$	−2	$x-3$	○
33	$3(x+1)$	x	$x+9$	1	$x+9$	○
34	$3(x+1)$	$x+1$	$4x+12$	4	$x+3$	○
35	$3(x+1)$	$x+2$	$7x+15$	1	$7x+15$	×

(4) 主ふるいの重複除去

表 2 から重複データを除くため、NO. 32 及び NO. 33 を削除する。

(5) 行列の作成

表 1 及び表 2 のふるい結果より表 3 の行列が得られる。

表 3. TBPS によるふるい結果の行列

NO.	素数基底		素イデアル基底	
	一次式値	素数分解	イデアル	素イデアル分解
1	133	$7\cdot 19$	$\theta-3$	$2^3\cdot 3$
2	134	$2\cdot 67$	$\theta-2$	7
3	135	$3^3\cdot 5$	$\theta-1$	2^2
4	136	$2^3\cdot 17$	θ	3^2
5	137	137	$\theta+1$	2^3
6	138	$2\cdot 3\cdot 23$	$\theta+2$	1
7	145	$5\cdot 29$	$\theta+9$	$2^3\cdot 3^3$
8	148	$3^2\cdot 37$	$\theta+12$	$3\cdot 7\cdot 19$
9	275	$5^2\cdot 11$	$2\theta+3$	$3\cdot 7$
10	406	$2\cdot 7\cdot 29$	$3\theta-2$	$3\cdot 19$
11	407	$11\cdot 37$	$3\theta-1$	$2^3\cdot 3^2$
12	409	409	$3\theta+1$	$2^2\cdot 3\cdot 7$
13	410	$2\cdot 5\cdot 41$	$3\theta+2$	3^4
14	416	$2^5\cdot 13$	$3\theta+8$	$3^2\cdot 7$
15	$137\cdot 407$	$2^{-3}\cdot 11\cdot 37\cdot 137$	1	1
16	$136\cdot 410$	$2^4\cdot 3^{-2}\cdot 5\cdot 17\cdot 41$	1	1
17	$136\cdot 409$	$-1\cdot 2^3\cdot 3\cdot 17\cdot 409$	$\theta-9$	$2^2\cdot 3^2\cdot 7$
18	$137\cdot 406$	$-1\cdot 2\cdot 7\cdot 29\cdot 137$	$\theta-7$	$2^3\cdot 19$
19	$136\cdot 407$	$-1\cdot 2^3\cdot 3^{-1}\cdot 11\cdot 17\cdot 37$	$\theta-3$	$2^3\cdot 3$
20	$3\cdot 135\cdot 137$	$-1\cdot 2^{-1}\cdot 3^4\cdot 5\cdot 137$	$\theta-3$	$2^3\cdot 3$
21	$135\cdot 409$	$-1\cdot 2^{-2}\cdot 3^3\cdot 5\cdot 409$	$\theta-2$	7
22	$134\cdot 409$	$-1\cdot 2\cdot 7^{-1}\cdot 67\cdot 409$	$\theta-1$	2^2
23	$3\cdot 135\cdot 138$	$2\cdot 3^5\cdot 5\cdot 23$	$\theta+3$	$2^2\cdot 3$
24	$3\cdot 137^2$	$2^{-2}\cdot 3\cdot 137^2$	$\theta+3$	$2^2\cdot 3$
25	$137\cdot 409$	$2^{-1}\cdot 137\cdot 409$	$\theta+5$	$2^3\cdot 7$
26	$3\cdot 136\cdot 137$	$2^3\cdot 3\cdot 17\cdot 137$	$\theta+9$	$2^3\cdot 3^3$
27	$3\cdot 136^2$	$-1\cdot 2^6\cdot 3\cdot 17^2$	$2\theta-9$	3^5
28	$3\cdot 135^2$	$-1\cdot 2^{-2}\cdot 3^7\cdot 5^2$	$2\theta-3$	3
29	$138\cdot 406$	$2^2\cdot 3\cdot 7\cdot 23\cdot 29$	$2\theta+5$	19
30	$135\cdot 410$	$-1\cdot 2\cdot 3^3\cdot 5^2\cdot 41$	$3\theta-7$	$2^2\cdot 3^3$
31	$135\cdot 407$	$-1\cdot 2^{-1}\cdot 3^3\cdot 5\cdot 11\cdot 37$	$3\theta-5$	$2^3\cdot 3$
32	$138\cdot 407$	$2\cdot 3\cdot 11\cdot 23\cdot 37$	$3\theta+7$	$2^3\cdot 3$
33	$137\cdot 410$	$2\cdot 5\cdot 41\cdot 137$	$3\theta+11$	$2^3\cdot 3^3$

表 3 に平方剰余を 6 個(R_1～R_6)追加し、各基底のベキに mod 2 を施して作成した 0-1 行列を示す。

表 4. TBPS により作成した 0-1 行列(A)

行番号	P_1, P_2, P_3, P_4, P_5 ～ P_{15}, P_{16}	Q_1～Q_4	R_1～R_6
1	0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0	1 1 0 0	1 0 0 1 1 1
2	0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0	0 0 1 0	1 0 1 1 1 0
3	0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0	0 1 0 0 1 0
4	0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0	0 0 0 0	1 0 1 1 1 0
5	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0	1 0 0 0	1 0 1 1 1 0
6	0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0	0 0 0 0	0 0 0 1 1 0
7	0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0	1 1 0 0	0 0 0 1 1 0
8	0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0	0 1 1 1	1 0 1 0 1 1
9	0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0	0 1 1 0	1 1 0 0 1 0
10	0 1 0 0 1 0 0 0 0 0 1 0 0 0 0 0	0 1 0 1	1 0 1 1 1 0
11	0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0	1 0 0 0	1 0 1 0 0 0
12	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1	0 1 1 0	1 1 1 0 0 1
13	0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0	0 0 0 0	1 1 0 0 1 1
14	0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0	0 0 1 0	1 1 0 1 1 1
15	0 1 0 0 0 1 0 0 0 0 0 1 0 0 1 0	0 0 0 0	0 0 0 0 0 0
16	0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0	0 0 0 0	0 0 0 0 0 0
17	1 1 0 0 0 0 0 1 0 0 0 0 0 0 0 1	0 0 1 0	0 1 1 0 1 1
18	1 1 0 0 1 0 0 0 0 0 1 0 0 0 1 0	1 0 0 1	0 0 1 0 1 0
19	1 1 1 0 0 1 0 1 0 0 0 1 0 0 0 0	1 1 0 0	1 0 0 1 1 1
20	1 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0	1 1 0 0	1 0 0 1 1 1
21	1 0 1 1 0 0 0 0 0 0 0 0 0 0 0 1	0 0 1 0	1 0 1 1 1 0
22	1 1 0 0 1 0 0 0 0 0 0 0 0 1 0 1	0 0 0 0	0 1 0 0 1 0
23	0 1 1 1 0 0 0 0 0 1 0 0 0 0 0 0	0 1 0 0	1 0 0 1 0 1
24	0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 0 0	1 0 0 1 0 1
25	0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1	1 0 1 0	1 1 0 0 1 1
26	0 1 1 0 0 0 0 1 0 0 0 0 0 0 1 0	1 1 0 0	0 0 0 1 1 0
27	1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 0 0	1 0 0 1 1 0
28	1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 0 0	0 1 1 0 1 0
29	0 0 1 0 1 0 0 0 0 1 1 0 0 0 0 0	0 0 0 1	0 0 0 1 0 0
30	1 1 1 0 0 0 0 0 0 0 0 0 1 0 0 0	0 1 0 0	0 0 0 0 1 0
31	1 1 1 1 0 1 0 0 0 0 0 1 0 0 0 0	1 1 0 0	1 0 1 1 1 0
32	0 1 1 0 0 1 0 0 0 1 0 1 0 0 0 0	1 1 0 0	0 0 0 0 0 0
33	0 1 0 1 0 0 0 0 0 0 0 0 1 0 1 0	1 1 0 0	0 0 0 1 1 1

4. 従属行の計算

単位行列をEとし、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 11 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 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3 3 <-- 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 3 4 5 6 7 8 9 0 1 2 3 <-- 列番号(1)
 25  | 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 1 1 0 0 0 1 0 1 1 0 0 0 0 0 0 0 0 0
 26  | 0 0 1 0 1 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 1 0 0 0 0 0 0 0 0
 27  | 0 1 1 0 0 1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 0 1 1 1 0 0 1 0 0 0 0 0 0 0
 28  | 0 1 0 1 0 1 1 1 1 0 0 0 0 0 1 0 1 1 0 0 0 1 1 1 0 0 0 1 0 0 0 0 0 0
 29  | 0 1 0 0 0 0 1 1 1 1 0 1 0 0 1 0 0 1 0 1 1 1 1 1 1 0 0 0 1 0 0 0 0 0
 30  | 0 1 0 1 0 0 1 1 1 0 1 1 1 0 1 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0
 31  | 0 1 0 1 0 1 1 1 1 1 1 0 0 0 1 0 1 0 0 0 1 1 1 0 1 0 0 0 0 0 1 0 0 0
 32  | 0 1 0 1 0 1 1 1 1 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 0 0
 33  | 0 0 1 1 0 1 0 0 0 1 1 0 1 0 0 0 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1
```

消去後のEの非ゼロが従属行の番号を示す。従属行は 9 組あり下記のようになる。

(a) 従属行 1： 6, 13, 16, 17, 21, 23, 24
(b) 従属行 2： 3, 5, 15, 19, 21, 25, 26
(c) 従属行 3： 2, 3, 6, 7, 8, 9, 17, 18, 19, 20, 22, 23, 24, 27
(d) 従属行 4： 2, 4, 6, 7, 8, 9, 15, 17, 18, 22, 23, 24, 28
(e) 従属行 5： 2, 7, 8, 9, 10, 12, 15, 18, 20, 21, 22, 23, 24, 25, 29
(f) 従属行 6： 2, 4, 7, 8, 9, 11, 12, 13, 15, 18, 19, 22, 30
(g) 従属行 7： 2, 4, 6, 7, 8, 9, 10, 11, 15, 17, 21, 22, 23, 25, 31
(h) 従属行 8： 2, 4, 6, 7, 8, 9, 11, 12, 15, 17, 18, 21, 22, 24, 32
(i) 従属行 9： 3, 4, 6, 10, 11, 13, 18, 19, 23, 33

5. 代数平方根の計算

各従属行は素イデアルふるいの結果を含んでいるため、代数平方根(イデアルの平方根) $H_k(M)$ を求める必要がある。このとき、従属行に含まれるイデアルから作成される関数 $F_k(\theta)$ は下記の様になる。

従属行 1: $F_1(\theta) = (\theta+2)(3\theta+2)(\theta-9)(\theta-2)(\theta+3)^2$

従属行 2: $F_2(\theta) = (\theta-1)(\theta+1)(\theta-3)(\theta-2)(\theta+5)(\theta+9)$

従属行 3: $F_3(\theta) = (\theta-2)(\theta-1)(\theta+2)(\theta+9)(\theta+12)(2\theta+3)(\theta-9)(\theta-7)$
$(\theta-3)^2(\theta-1)(\theta+3)^2(2\theta-9)$

従属行 4: $F_4(\theta) = (\theta-2)\theta(\theta+2)(\theta+9)(\theta+12)(2\theta+3)(\theta-9)(\theta-7)(\theta-1)$
$(\theta+3)^2(2\theta-3)$

従属行 5: $F_5(\theta)=(\theta-2)(\theta+9)(\theta+12)(2\theta+3)(3\theta-2)(3\theta+1)(\theta-7)(\theta-3)$
$(\theta-2)(\theta-1)(\theta+3)^2(\theta+5)(2\theta+5)$

従属行 6: $F_6(\theta)=(\theta-2)\theta(\theta+9)(\theta+12)(2\theta+3)(3\theta-1)(3\theta+1)(3\theta+2)(\theta-7)$
$(\theta-3)(\theta-1)(3\theta-7)$

従属行 7: $F_7(\theta)=(\theta-2)\theta(\theta+2)(\theta+9)(\theta+12)(2\theta+3)(3\theta-2)(3\theta-1)(\theta-9)$
$(\theta-2)(\theta-1)(\theta+3)(\theta+5)(3\theta-5)$

従属行 8: $F_8(\theta)=(\theta-2)\theta(\theta+2)(\theta+9)(\theta+12)(2\theta+3)(3\theta-1)(3\theta+1)(\theta-9)$
$(\theta-7)(\theta-2)(\theta-1)(\theta+3)(3\theta+7)$

従属行 9: $F_9(\theta)=(\theta-1)\theta(\theta+2)(3\theta-2)(3\theta-1)(3\theta+2)(\theta-7)(\theta-3)(\theta+3)(3\theta+11)$

$f(\theta)=3\theta^2+2\theta-9,\ f(M)\equiv 0 \pmod N$ の関係を使用し、$H_k(\theta)=F_k(\theta)^{1/2}$ を求める。

これは、直接求まらないので、下記のようにして求める。ここで、m は $F_k(\theta)$ を作成する、θ の一次式の数である。

$$3\cdot B_k(\theta)^2\equiv 3^{m-1}F_k(\theta) \pmod{f(\theta)}$$

から、非線形連立一次方程式を経由し $B_k(\theta)$ を求める。次に下記で $H_k(M)$ を求める。

$$H_k(M)\equiv B_k(M)\cdot D^{(m-2)/2} \pmod N,\quad D\equiv 1/3\equiv 18584 \pmod N$$

具体的に計算すると下記のようになる。

従属行 1: $3^2\cdot F_1(\theta)\equiv 124740\theta+265356,\ B_1(\theta)\equiv 99\theta+243,\ H_1(M)\equiv 1523$

従属行 2: $3^2\cdot F_2(\theta)\equiv -93632\theta+149184,\ B_2(\theta)\equiv 76\theta-180,\ H_2(M)\equiv 7323$

従属行 3: $3^6\cdot F_3(\theta)\equiv -22934099363 84\theta+9212064777216,$
$B_3(\theta)\equiv 214256\theta-1712592,\ H_3(M)\equiv 15979$

従属行 4: $3^5\cdot F_4(\theta)\equiv -570102848\theta+20944155456,$
$B_4(\theta)\equiv 47572\theta+13860,\ H_4(M)\equiv 19340$

従属行 5: $3^6\cdot F_5(\theta)\equiv -19909037998 08\theta+22070523589632,$
$B_5(\theta)\equiv 1556016\theta+305424,\ H_5(M)\equiv 5487$

従属行 6: $3^5\cdot F_6(\theta)\equiv -110965863375536\theta+16006016565504,$
$B_6(\theta)\equiv 966168\theta-1592136,\ H_6(M)\equiv 23326$

従属行 7: $3^6\cdot F_7(\theta)\equiv -74682339863 04\theta+11716954373376,$
$B_7(\theta)\equiv 689976\theta-1573992,\ H_7(M)\equiv 6111$

従属行 8: $3^6 \cdot F_8(\theta) \equiv 83655475384 32\theta + 20979815463936,$
$B_8(\theta) \equiv 636048\theta + 2404080,\ H_8(M) \equiv 13635$

従属行 9: $3^4 \cdot F_9(\theta) \equiv 1511654 40\theta + 952342272,$
$B_9(\theta) \equiv 9720\theta + 5832,\ H_9(M) \equiv 16392$

6. 因数分解結果

(1) 従属行 1：6,13,16,17,21,23,24

表 3 に従属行を当てはめ、N=55751 を法とすると素数基底で下記の関係が成立する。

$(2^3 \cdot 3^4 \cdot 5^2 \cdot 17 \cdot 23 \cdot 41 \cdot 137 \cdot 409)^2 \equiv 1 \pmod{55751}$

上記と代数平方根の値が 1523 となることから下記が成立する。

$1523^2 \equiv 1523^2 \pmod{5571}$

これは自明解のため分解できない。

(2) 従属行 2：3,5,15,19,21,25,26

表 3 に従属行を当てはめ、N=55751 を法とすると素数基底で下記の関係が成立する。

$(3^3 \cdot 5 \cdot 11 \cdot 17 \cdot 37 \cdot 137^2 \cdot 409)^2 \equiv 1 \pmod{55751}$

上記と代数平方根の値が 7323 となることから下記が成立する。

$7323^2 \equiv 7323^2 \pmod{5571}$

これは自明解のため分解できない。

(3) 従属行 3：2,3,6,7,8,9,17,18,19,20,22,23,24,27

表 3 に従属行を当てはめ、N=55751 を法とすると素数基底で下記の関係が成立する。

$(2^8 \cdot 3^7 \cdot 5^3 \cdot 11 \cdot 17^2 \cdot 23 \cdot 29 \cdot 37 \cdot 67 \cdot 137 \cdot 409)^2 \equiv 1 \pmod{55751}$

上記と代数平方根の値が 15979 となることから下記が成立する。

$8055^2 \equiv 15979^2 \pmod{55751}$

従って下記のようになる。

GCD(15979-8055,55751)=283, GCD(15979+8055,55751)=197

即ち、55751=197・283 と分解される。

(4) 従属行 4：2,4,6,7,8,9,15,17,18,22,23,24,28

同様に下記が成立する。

$8111^2 \equiv 19340^2 \pmod{55751}$

従って 55751=197・283 と分解される。

(5) 従属行 5：2,7,8,9,10,12,15,18,20,21,22,23,24,25,29

同様に下記が成立する。

$10864^2 \equiv 5487^2 \pmod{55751}$

従って 55751=197・283 と分解される。

(6) 従属行 6：2,4,7,8,9,11,12,13,15,18,19,22,30

同様に下記が成立する。

$4648^2 \equiv 23326^2 \pmod{55751}$

従って 55751=197･283 と分解される。

(7) 従属行 7：2,4,6,7,8,9,10,11,15,17,21,22,23,25,31

同様に下記が成立する。

$398^2 \equiv 6111^2 \pmod{55751}$

従って 55751=197･283 と分解される。

(8) 従属行 8：2,4,6,7,8,9,11,12,15,17,18,21,22,24,32

同様に下記が成立する。

$26834^2 \equiv 13635^2 \pmod{55751}$

従って 55751=197･283 と分解される。

(9) 従属行 9：3,4,6,10,11,13,18,19,23,33

同様に下記が成立する。

$16392^2 \equiv 16392^2 \pmod{55751}$

これは自明解のため分解できない。