2 次の DBPS2 にふるい例 1

2006/10/24　後 保範

1. 概要

2 次多項式を使用した DBPS(Double Base Polynomial Sieve, 2 重基底多項式篩法)の改訂版(DBPS2, Double Base Polynomial Sieve 2nd, 改訂 2 重基底多項式篩法)である。

N を分解対象数とするとき、 $f_k(x)=A_kx^2+B_kx+C_k,\ f(M_k)\equiv 0 \pmod N$ となる複数個$(k=1,2,\cdots,L)$の多項式 $f_k(x)$ と整数 M_k を求める。

次に、一定の範囲の整数 a_k,b_k に対して、下記で s_kx+t_k を計算する。

$$S_kx+T_k=(\alpha_kx+a_k)\cdot(\beta_kx+b_k)-f_k(x)$$
$$S_k=\beta_ka_k+\alpha_kb_k-B_k,\ T_k=a_kb_k-C_k,\ A_k=\alpha_k\cdot\beta_k \qquad \text{---- (1)}$$
$$G_k=sign(S_k)\cdot GCD(|S_k|,|T_k|),\ s_k=S_k/G_k,\ t_k=T_k/G_k$$

このとき、s_kx+t_k が同一で G_k が異なるもの及び、s_kx+t_k が α_kx+a_k 又は β_kx+b_k と一致するものを、α_kx+a_k 、β_kx+b_k 及び s_kx+t_k を分解する素数基底の個数以上ふるいで集める。

このふるい処理において、イデアル $\alpha_k\theta+a_k$ 及び $\beta_k\theta+b_k$ が素イデアル基底で分解できるものを使用するのが、DBPS2 の特徴である。それは、素イデアル基底で分解できるものを使用すると、S_kx+T_k もまた素イデアル基底で分解でき、G_k だけ異なり、s_kx+t_k が同じとなるものが多く発生し、ふるいの効率が向上するためである。

DBPS2 は TBPS2 と異なり、素イデアル基底は整数 a_k,b_k の選定にだけ使用し、ふるいには使用しないで、素数基底(途中で追加あり)だけを使用してふるいをおこなう。

2. 計算対象

$N=55751$ を DBPS2 で因数分解する。

ふるいには下記の 3 つの関数を使用する。

$$f_1(x)=3x^2+2x-9,\quad f_1(M_1)\equiv 0 \pmod N,\ M_1=136$$
$$f_2(x)=2x^2-27,\quad f_2(M_2)\equiv 0 \pmod N,\ M_2=167$$
$$f_3(x)=x^2+55,\quad f_3(M_3)\equiv 0 \pmod N,\ M_3=236$$

3. 素数基底(P)の設定

3.1 基本素数基底(P1)

基本素数基底 P1 は小さい順に 10 番目までの素数と-1 で構成する。

即ち、P1 は下記のようになる。

P1 = {-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29}

3.2 素イデアル基底(Q_k)

イデアル基底は $f_k(x)$ ごとに定義される。

イデアル基底 Q_k は $f_k(v_{kj}) \equiv 0 \pmod{p_j}$ となる p_j と v_{kj} の組みで表される。

ここでは、$p_1 = 2,\ p_2 = 3,\ p_3 = 5$ の 3 つを使用する。

(1) Q1 ($f_1(x)$ に対応する素イデアル基底)

Q1 = { (2;1), (3;0) }

(2) Q2 ($f_2(x)$ に対応する素イデアル基底)

Q2 = { (2;0), (3;0), (5;1,4) }

(3) Q3 ($f_3(x)$ に対応する素イデアル基底)

Q3 = {(2;1), (5;4) }

3.3 素イデアル基底による分解

$f_k(x) = A_k x^2 + B_k x + C_k$ のイデアル $a\theta + b$ が素イデアル q (p;v)で割れるとは、N(a,b) が p で割れることである(高速計算は別の方法)。従って、各 $f_k(x)$ において、一定区間のイデアルが素イデアル Qk で完全に分解され、対応イデアルの θ を M_k で置き換えた値が基本素数基底 P1 で完全には分解できないものは下記のようになる。

(1) $3\theta + a_1, \theta + b_1$ の Q1 での分解

(a) $|a_1| \le 5$ において $3\theta + a_1$ が Q1 で分解でき、$3M_1 + a_1$ が P1 で分解できないもの

$3\theta - 5$ → P1 以外の因数は 31

$3\theta - 4$ → P1 以外の因数は 101

$3\theta - 1$ → P1 以外の因数は 37

$3\theta + 2$ → P1 以外の因数は 41

$3\theta + 3$ → P1 以外の因数は 137

$3\theta + 5$ → P1 以外の因数は 59

(b) $|b_1| \le 2$ において $\theta + b_1$ が Q1 分解でき、$M_1 + b_1$ が P1 で分解できないもの

$\theta + 1$ → P1 以外の因数は 137

(2) $2\theta + a_2, \theta + b_2$ の Q2 での分解

(a) $|a_2| \le 4$ において $2\theta + a_2$ が Q2 分解でき、$2M_2 + a_2$ が P1 で分解できないもの

$2\theta - 3$ → P1 以外の因数は 331

$2\theta - 2$ → P1 以外の因数は 83

2θ → P1 以外の因数は 167

$2\theta + 3$ → P1 以外の因数は 337

(b) $|b_2| \leq 2$ において $\theta + b_2$ が Q2 分解でき、$M_2 + b_2$ が P1 で分解できないもの

$\theta - 1$ → P1 以外の因数は 83

θ → P1 以外の因数は 167

(3) $\theta + a_3$ の Q3 での分解

(a) $|a_3| \leq 4$ において $\theta + a_3$ が Q3 分解でき、$M_3 + a_3$ が P1 で分解できないもの

$\theta - 3$ → P1 以外の因数は 233

$\theta + 3$ → P1 以外の因数は 239

3.4 追加素数基底(P2)と素数基底(P)

3.3 節で求めた P1 以外の因数から重複を除いたものを追加素数基底 P2 とする。

すると、P2 は下記の様に 12 個となる。

P2 = { 31, 37, 41, 59, 83, 101, 137, 167, 233, 239,331, 337 }

素数基底 P は P1 と P2 を合わせたもので、下記のようになる 23 個となる。

P = {-1,2,3,5,7,11,13,17,19,23,29, 31,37,41,59,83,101,137,167,233,239,331,337 }

4. ふるいの準備

$S_k x + T_k = (\alpha_k x + a_k) \cdot (\beta_k + b_k) - f_k(x)$ を使用してふるいをおこなう前に、ふるいに使用する 1 次式 $\alpha_k x + a_k$ と $\beta_k + b_k$ を選定し、素数基底 P で分解しておく。ふるいに使用するものは、素数基底 P で分解できるものである。a_k, b_k の区間は 3.3 節のものを使用する。

4.1 $f_1(x)$ に対する 1 次式

$f_1(x)$ に対するふるいに使用する 1 次式は表 1 のようになる。

表 1. ふるいに使用する $3x + a_1$ 及び $x + b_1$ (M_1=136)

項番	$3x + a_1$	値($3M_1+a_1$)	$3M_1+a_1$ の P での分解
1	3x − 5	403	13·31
2	3x − 4	404	2^2·101
3	3x − 3	405	3^4·5
4	3x − 2	406	2·7·29
5	3x − 1	407	11·37
6	3x	408	2^3·3·17
7	3x + 2	410	2·5·41
8	3x + 3	411	3·137
9	3x + 5	413	7·59
項番	$x + b_1$	値(M_1+b_1)	M_1+b_1 の P での分解
1	x − 1	135	3^3·5
2	x	136	2^3·17
3	x + 1	137	137

4	x + 2	138	2·3·23

4.2 $f_2(x)$ に対する 1 次式

$f_2(x)$ に対するふるいに使用する 1 次式は表 2 のようになる。

表 2. ふるいに使用する $2x+a_2$ 及び $x+b_2$ (M_2=167)

項番	$2x + a_2$	値($2M_2+a_2$)	$2M_2+a_2$ の P での分解
1	2x − 4	330	2·3·5·11
2	2x − 3	331	331
3	2x − 2	332	2^2·83
4	2x − 1	333	3^2·37
5	2x	334	2·167
6	2x + 2	336	2^4·3·7
7	2x + 3	337	337
8	2x + 4	338	2·13^2
項番	$x + b_2$	値(M_2+b_2)	M_2+b_2 の P での分解
1	x − 2	165	3·5·11
2	x − 1	166	2·83
3	x	167	167
4	x + 1	168	2^3·3·7
5	x + 2	169	13^2

4.3 $f_3(x)$ に対する 1 次式

$f_3(x)$ に対するふるいに使用する 1 次式は表 3 のようになる。

表 3. ふるいに使用する $x+a_3$ (M_3=236)

項番	$x + a_3$	値(M_3+a_3)	M_3+a_3 の P での分解
1	x − 4	232	2^3·29
2	x − 3	233	233
3	x − 2	234	2·3^2·13
4	x	236	2^2·59
5	x + 2	238	2·7·17
6	x + 3	239	239
7	x + 4	240	2^4·3·5

5. ふるい

式(1)を使用して各 $f_k(x)$ に対するふるいをおこなう。ふるいに使用する 1 次式は $f_k(x)$ ごとに 4 章で作成したものを使用し、$|s_k| \leq 2$ となるものだけ採用する。

ふるいは S_k が 0,±1,±2,… となる順に行い、詳細は $f_k(x)$ ごとに定める。このとき、a_k は上昇順に b_k は下降順に動かして、1 個又は 2 個前の T_k が同一なら同一となったもの以

降は重複のため、ふるい対象から除外する。

5.1 $f_1(x)$に対するふるい

$S_1 = 0,\pm1,\pm2,\pm3,\pm4,\pm6,\pm8$ となる順におこなったふるい結果を表 4 に示す。

ここで、表 4 中の $S_1, a_1, b_1, G_1, s_1, t_1$ は下記の式中の記号に対応する。

$$S_1 x + T_1 = (3x + a_1) \cdot (x + b_1) - f_1(x)$$

$$S_1 = a_1 + 3b_1 - 2,\ T_1 = a_1 b_1 + 9$$

$$G_1 = sign(S_1) \cdot GCD(|S_1|, |T_1|),\ s_1 = S_1 / G_1,\ t_1 = T_1 / G_1$$

表 4. $f_1(x)$における DBPS2 のふるい結果

番号	S_1	a_1	b_1	G_1	s_1	t_1
1	0	5	-1	1	0	4
2	0	2	0	1	0	9
3	0	-1	1	1	0	8
4	0	-4	2	1	0	1
5	1	3	0	1	1	9
6	-1	-2	1	-1	1	-7
7	-1	-5	2	-1	1	1
8	2	-2	2	1	2	5
9	-2	3	-1	-2	1	-3
10	-2	0	0	-1	2	-9
11	3	5	0	3	1	3
12	-3	-1	0	-3	1	-3
13	4	3	1	4	1	3
14	-4	-5	1	-4	1	-1
15	-6	-4	0	-3	2	-3
16	-8	-3	-1	-4	2	-3

5.2 $f_2(x)$ に対するふるい

$S_2 = 0,\pm1,\pm2,\pm3$ となる順におこなったふるい結果を表 5 に示す。

ここで、表 5 中の $S_2, a_2, b_2, G_2, s_2, t_2$ は下記の式中の記号に対応する。

$$S_2 x + T_2 = (2x + a_2) \cdot (x + b_2) - f_2(x)$$

$$S_2 = a_2 + 2b_2,\ T_2 = a_2 b_2 + 27$$

$$G_2 = sign(S_2) \cdot GCD(|S_2|, |T_2|),\ s_2 = S_2 / G_2,\ t_2 = T_2 / G_2$$

表 5. $f_2(x)$における DBPS2 のふるい結果

番号	S_2	a_2	b_2	G_2	s_2	t_2
1	0	4	-2	1	0	19
2	0	2	-1	1	0	25
3	0	0	0	1	0	27
4	1	3	-1	1	1	24

5	1	-1	1	1	1	26
6	1	-3	2	1	1	21
7	-1	3	-2	-1	1	-21
8	-1	-1	0	-1	1	-27
9	-1	-3	1	-1	1	-24
10	2	4	-1	1	2	23
11	2	2	0	1	2	27
12	-2	2	-2	-1	2	-23
13	-2	0	-1	-1	2	-27
14	3	3	0	3	1	9
15	-3	-3	0	-3	1	-9

5.3 $f_3(x)$ に対するふるい

$S_3 = 0,\pm1,\pm2$ となる順におこなったふるい結果を表 6 に示す。

ここで、表 6 中の $S_3, a_3, b_3, G_3, s_3, t_3$ は下記の式中の記号に対応する。

$$S_3 x + T_3 = (x + a_3)\cdot(x + b_3) - f_3(x)$$

$$S_3 = a_3 + b_3,\ T_3 = a_3 b_3 - 55$$

$$G_3 = sign(S_3)\cdot GCD(|S_3|,|T_3|),\ s_3 = S_3 / G_3,\ t_3 = T_3 / G_3$$

表 6. $f_3(x)$ における DBPS2 のふるい結果

番号	S_3	a_3	b_3	G_3	s_3	t_3
1	0	4	-2	1	0	19
2	0	2	-1	1	0	25
3	0	0	0	1	0	27
4	1	3	-1	1	1	24
5	1	-1	1	1	1	26
6	1	-3	2	1	1	21
7	-1	3	-2	-1	1	-21
8	-1	-1	0	-1	1	-27
9	-1	-3	1	-1	1	-24
10	2	4	-1	1	2	23
11	2	2	0	1	2	27
12	-2	2	-2	-1	2	-23

6. 重複データの削除

重複データの削除は、各 $f_k(x)$ に対するふるいに対して行い、$G_k, s_k x + t_k$ が同一なもの及び $s_k x + t_k$ が $\alpha_k x + a_k$ 又は $\beta_k + b_k$ と一致するものに対して行う。そのため、各 $f_k(x)$ に対するふるい結果を s_k, t_k, G_k でソートしておく。今回は $G_k, s_k x + t_k$ が同一なものは存在しないので、$s_k x + t_k$ が $\alpha_k x + a_k$ 又は $\beta_k + b_k$ と一致するものに対して行う。これに該当するデータは $f_1(x)$ に対するふるいにだけ存在する。

6.1 $f_1(x)$に対する重複データの削除

$|s_1| \leq 2$ なので表 8 から s_1x+t_1 が表 1 の x_1+b_1 と一致するものを求めると、表 7 が得られる。

表 7. $f_1(x)$のふるい結果でs_1x+t_1がx_1+b_1と一致するもの

番号	a_1	b_1	G_1	s_1	t_1
1	-5	1	-4	1	-1
2	-5	2	-1	1	1

このデータは互いに乗算した結果が他のデータに一致しないので、重複削除の対象とはならない。

7. ふるいデータの選定

6 章のふるい結果で得られたデータで、6 章で削除されなかったものを対象にする。データ選定は 2 つの方法でおこなう。最初に、$s_kM_k+t_k$ が素数基底 P で分解されるものを選定する。これにより選定されたものを 1 の区分にする。ただし、s_1x+t_1 が x_1+b_1 に一致したものは 3 の区分にし、No.は区分 1 と区分 2 の後にする。次に、G_k が異なり、$s_kM_k+t_k$ が一致するものを選択する。これにより選定されたものを 2 の区分にする。これらの処理をおこなう前に、データはs_k, t_k, G_k でソートしておく。選定からもれたものは表から取り除くが、ここではどれが選定されたデータか分かり易くするため、0 の区分にして表に残しておく。また、次の行列作成のため、1 と 3 の区分のものは素数基底で因数分解しておく。また、No.は行列作成時の行番号に対応する。

7.1 $f_1(x)$に対するふるいデータの選定

表 8 に $f_1(x)$ に対するふるい結果で行列作成用に選択されたものを示す。
区分が 1,2 及び 3 のデータが選択されたもので、0 は選択されないものである。

表 8. $f_1(x)$に対するふるいデータからの選定結果

No.	a_1	b_1	G_1	s_1	t_1	区分	$s_1M_1+t_1$	
							値	P の分解
1	-4	2	1	0	1	1	1	1
2	5	-1	1	0	4	1	4	2^2
3	-1	1	1	0	8	1	8	2^3
4	2	0	1	0	9	1	9	3^2
---	-2	1	-1	1	-7	0	129	-----
5	-1	0	-3	1	-3	1	133	$7\cdot 19$
6	3	-1	-2	1	-3	1	133	$7\cdot 19$
10	-5	1	-4	1	-1	3	135	$3^3\cdot 5$
11	-5	2	-1	1	1	3	137	137
7	5	0	3	1	3	2	139	-----
7	3	1	4	1	3	2	139	-----

8	3	0	1	1	9	1	145	$5\cdot 29$
---	0	0	-1	2	-9	0	263	-----
9	-3	-1	-4	2	-3	2	269	-----
9	-4	0	-3	2	-3	2	269	-----
---	-2	2	1	2	5	0	277	-----

7.2 $f_2(x)$ に対するふるいデータの選定

表 9 に $f_2(x)$ に対するふるい結果で行列作成用に選択されたものを示す。区分が 1 のデータが選択されたもので、0 は選択されないものである。

表 9. $f_2(x)$ に対するふるいデータからの選定結果

No.	a_2	b_2	G_2	s_2	t_2	区分	$s_2M_2+t_2$	
							値	P の分解
12	4	-2	1	0	19	1	19	19
13	2	-1	1	0	25	1	25	5^2
14	0	0	1	0	27	1	27	3^3
15	-1	0	-1	1	-27	1	140	$2^2\cdot 5\cdot 7$
16	-3	1	-1	1	-24	1	143	$11\cdot 13$
---	3	-2	-1	1	-21	0	146	-----
---	-3	0	-3	1	-9	0	158	-----
17	3	0	3	1	9	1	176	$2^4\cdot 11$
---	-3	2	1	1	21	0	188	-----
---	3	-1	1	1	24	0	191	-----
---	-1	1	1	1	26	0	193	-----
---	0	-1	-1	2	-27	0	307	-----
---	2	-2	-1	2	-23	0	311	-----
18	4	-1	1	2	23	1	357	$3\cdot 7\cdot 17$
19	2	0	1	2	27	1	361	19^2

7.3 $f_3(x)$ に対するふるいデータの選定

表 10 に $f_3(x)$ に対するふるい結果で行列作成用に選択されたものを示す。区分が 1 のデータが選択されたもので、0 は選択されないものである。

表 10. $f_3(x)$ に対するふるいデータからの選定結果

No.	a_3	b_3	G_3	s_3	t_3	区分	$s_3M_3+t_3$	
							値	P の分解
20	0	0	-1	0	55	1	55	$5\cdot 11$
21	2	-2	-1	0	59	1	59	59
22	3	-3	-1	0	64	1	64	2^6
---	4	-4	-1	0	71	0	71	-----
23	4	-3	1	1	-67	1	169	13^2
24	3	-2	1	1	-61	1	175	$5^2\cdot 7$

25	2	-3	-1	1	61	1	297	$3^3 \cdot 11$
26	3	-4	-1	1	67	1	303	$3 \cdot 101$
---	4	-2	1	2	-63	0	409	-----
---	2	0	1	2	-55	0	417	-----
27	0	-2	-1	2	55	1	527	$17 \cdot 31$
---	2	-4	-1	2	63	0	535	-----

8. 行列作成

8.1 ふるい結果による行列作成

表 8,表 9,表 10 の選定されたデータに対して、表 1,表 2,表 3 を使用して、素数基底の番号を列番号に、データ No.を行番号にした 27×23 次元の行列を作成する。区分が 1 及び 3 の各データに対して、左辺 $(\alpha_k M_k + a_k)\cdot(\beta_k M_k + b_k)$ の素数基底 P で分解しそのベキ指数を正で、右辺 $G_k \cdot (s_k M_k + t_k)$ も同じくベキ指数を負で、対応素数番号の位置に入れる。一方、区分が 2 のデータに対しては、ペアーとなる 1 組のデータで 1 行を作成する。ペアーとなる左辺 $(\alpha_k M_k + a_k)\cdot(\beta_k M_k + b_k)$ は素数基底 P で分解し、前のデータのベキ指数は負で、後のデータのベキ指数は正で対応素数番号の位置に入れる。更に、ベアーとなる右辺は G_k だけを素数基底 P で分解し、前のデータのベキ指数は正で、後のデータのベキ指数は負として左辺とは逆の符号で入れる。

例で示すと、表 8 の No.2 のデータは $(3M_1 + 4)\cdot(M_1 - 2) \equiv 2^2 \pmod N$ であり、これに $M_1 = 136$ を代入すると $413 \cdot 135 \equiv 2^2 \pmod N$、即ち $3^3 \cdot 5 \cdot 7 \cdot 59 \equiv 2^2 \pmod N$ となる。素数基底 P の k 番目の素数を p_k とすると、p_2=2、p_3=3、p_4=5、p_5=7、p_{15}=59 となるため表 11 の No.2 のデータが得られる。

また区分 2 のデータの例では、表 8 の No.7 の 2 つのデータは下記となる。

$$(3M_1 + 5)\cdot M_1 \equiv 3\cdot(M_1 + 3) \pmod N$$

$$3\cdot(M_1 + 1)^2 \equiv 4\cdot(M_1 + 3) \pmod N$$

この両式から $(M_1 + 3)$ を消去し、$M_1 = 136$ を代入すると次式が得られる。

$$3^2 \cdot 137^2 \equiv 4 \cdot 413 \cdot 136 \pmod N$$

これを因数分解すると次式が得られる。

$$3^2 \cdot 137^2 \equiv 2^5 \cdot 7 \cdot 17 \cdot 59 \pmod N$$

素数基底 P の k 番目の素数を p_k とすると、p_2=2、p_3=3、p_5=7、p_8=17、p_{15}=59、p_{18}=137 となるため表 11 の No.7 のデータが得られる。

表 11 に作成した行列を示す。素数基底 P の番号は小さい順に対応する。即ち、1 番は-1 で、2 番は素数の 2、3 番は素数の 3 で、以下順に 23 番は 337 に対応する。

表 11. DBPS2 のふるいにより作成された行列

No.	素数基底 P の番号(1～23)																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	0	3	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0

2	0	-2	3	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
3	0	-3	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
4	0	4	-2	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
5	1	3	-1	0	-1	1	0	1	-1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
6	1	-1	4	1	-1	0	0	0	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	0
7	0	-5	2	0	-1	0	0	-1	0	0	0	0	0	0	-1	0	0	2	0	0	0	0	0
8	0	3	1	-1	0	0	0	1	0	0	-1	0	0	0	0	0	0	1	0	0	0	0	0
9	0	7	-8	-2	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
10	1	-2	-3	-1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
11	1	1	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0	-1	0	0	0	0	0
12	0	1	1	1	0	1	2	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	5	1	-2	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
14	0	1	-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0
15	1	-2	2	-1	-1	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
16	1	3	1	0	1	-1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
17	0	-4	-1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
18	0	2	-1	0	-1	0	2	-1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
19	0	4	1	0	1	0	0	0	-2	0	0	0	0	0	0	0	0	0	1	0	0	0	0
20	1	4	0	-1	0	-1	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0
21	1	2	2	0	1	0	1	1	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0
22	1	-6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0
23	0	4	1	1	0	0	-2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
24	0	1	2	-2	-1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
25	1	1	-3	0	1	-1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
26	1	3	-1	0	0	0	0	0	0	0	1	0	0	0	0	0	-1	0	0	0	1	0	0
27	1	3	2	0	0	0	1	-1	0	0	0	-1	0	0	1	0	0	0	0	0	0	0	0

8.2 行列の縮小

表 11 の各列の絶対値の合計を求め、合計値が 1 以下に対応する素数を素数基底 P から除くと行列のサイズが小さくなる。このとき、同時に除外した素数のベキが 0 でない行も除く必要がある。ここでは、素数基底 P の 14 番目、22 番目及び 23 番目の素数、41、331 及び 337 を除き、これに対応して 4 行、16 行及び 17 行のデータを削除する。従って、素数基底 P は 20 個で下記のようになる。これに再度 1 から番号を付ける。

P = {-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 59 ,83, 101, 137, 167, 233, 239}

縮小した 24×20 次元の行列を表 12 に示す。

表 12. 縮小した行列

No	縮小した素数基底 P の番号(1～20)																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0	3	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
2	0	-2	3	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
3	0	-3	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0
4	1	3	-1	0	-1	1	0	1	-1	0	0	0	1	0	0	0	0	0	0	0

5	1	-1	4	1	-1	0	0	0	-1	0	0	0	0	0	0	0	1	0	0	0
6	0	-5	2	0	-1	0	0	-1	0	0	0	0	0	-1	0	0	2	0	0	0
7	0	3	1	-1	0	0	0	1	0	0	-1	0	0	0	0	0	1	0	0	0
8	0	7	-8	-2	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
9	1	-2	-3	-1	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0
10	1	1	1	0	0	0	1	0	0	1	0	1	0	0	0	0	-1	0	0	0
11	0	1	1	1	0	1	2	0	-1	0	0	0	0	0	0	0	0	0	0	0
12	0	5	1	-2	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
13	0	1	-3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0
14	1	-2	2	-1	-1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0
15	0	2	-1	0	-1	0	2	-1	0	0	0	0	0	0	1	0	0	0	0	0
16	0	4	1	0	1	0	0	0	-2	0	0	0	0	0	0	0	0	1	0	0
17	1	4	0	-1	0	-1	0	0	0	0	0	0	0	2	0	0	0	0	0	0
18	1	2	2	0	1	0	1	1	0	0	0	0	0	-1	0	0	0	0	0	0
19	1	-6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
20	0	4	1	1	0	0	-2	0	0	0	0	0	0	0	0	0	0	0	1	0
21	0	1	2	-2	-1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
22	1	1	-3	0	1	-1	0	1	0	0	0	0	0	0	0	0	0	0	1	0
23	1	3	-1	0	0	0	0	0	0	0	1	0	0	0	0	-1	0	0	0	1
24	1	3	2	0	0	0	1	-1	0	0	0	-1	0	1	0	0	0	0	0	0

9. 因数分解

「2 次の DBPS2 による因数分解例 1」を参照。