2 次の DBPS2 にふるい例 2

2006/11/03　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

$N=18689147$ を DBPS2 で因数分解する。

ふるいには下記の 4 つの関数を使用する。

$$f_1(x)=7x^2-3x+180,\qquad f_1(M_1)\equiv 0 \pmod N,\ M_1=2311$$
$$f_2(x)=10x^2+7x-127,\qquad f_2(M_2)\equiv 0 \pmod N,\ M_2=1933$$
$$f_3(x)=11x^2-4x-85,\qquad f_3(M_3)\equiv 0 \pmod N,\ M_3=3193$$
$$f_4(x)=13x^2-9x+150,\qquad f_4(M_4)\equiv 0 \pmod N,\ M_4=1696$$

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 30 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,　31, 37, 41, 43, 47, 53, 59, 61, 67, 71,
73, 79, 83, 89, 97, 101, 103, 107, 109, 113 }

3.2 素イデアル基底(Qk)

イデアル基底は $f_k(x)$ ごとに定義される。

イデアル基底 Qk 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、 $p_1 = 2,\ p_2 = 3,\ p_3 = 5, p_4 = 7, p_5 = 11$ の 5 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;0,1), (3;0), (5;0,4), (7;4) }
(2) Q2 ($f_2(x)$ に対応する素イデアル基底)
Q2 = { (2;1), (5;1), (11;1,6) }
(3) Q3 ($f_3(x)$ に対応する素イデアル基底)
Q3 = {(2;1), (3;1), (5;0,4), (7;2,6), (11;9) }
(4) Q4 ($f_4(x)$ に対応する素イデアル基底)
Q4 = {(2;0,1), (3;0), (5;0,3), (7;1,4), (11;1,9) }

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) $7\theta + a_1, \theta + b_1$ の Q1 での分解
(a) $|a_1| \le 25$ のとき $7\theta + a_1$ が Q1 で分解でき、$7M_1 + a_1$ が P1 で分解できないもの
$7\theta - 24$ → P1 以外の因数は 557
$7\theta - 20$ → P1 以外の因数は 151
$7\theta - 15$ → P1 以外の因数は 8081
$7\theta - 3$ → P1 以外の因数は 8087
7θ → P1 以外の因数は 2311
$7\theta + 12$ → P1 以外の因数は 16187
$7\theta + 17$ → P1 以外の因数は 2699
$7\theta + 25$ → P1 以外の因数は 8101
(b) $|b_1| \le 12$ のとき $\theta + b_1$ が Q1 分解でき、$M_1 + b_1$ が P1 で分解できないもの
$\theta - 9$ → P1 以外の因数は 1151

$\theta-4$ → P1 以外の因数は 769

θ → P1 以外の因数は 2311

$\theta+6$ → P1 以外の因数は 331

(2) $5\theta+a_2, 2\theta+b_2$ の Q2 での分解

(a) $|a_2|\leq 22$ のとき $5\theta+a_2$ が Q2 分解でき、$5M_2+a_2$ が P1 で分解できないもの

$5\theta-16$ → P1 以外の因数は 9649

$5\theta-15$ → P1 以外の因数は 193

$5\theta+1$ → P1 以外の因数は 179

$5\theta+6$ → P1 以外の因数は 509

$5\theta+20$ → P1 以外の因数は 149

$5\theta+21$ → P1 以外の因数は 167

(b) $|b_2|\leq 16$ のとき $2\theta+b_2$ が Q2 分解でき、$2M_2+b_2$ が P1 で分解できないもの

$2\theta-7$ → P1 以外の因数は 227

$2\theta-6$ → P1 以外の因数は 193

$2\theta-1$ → P1 以外の因数は 773

$2\theta+1$ → P1 以外の因数は 1289

$2\theta+8$ → P1 以外の因数は 149

$2\theta+13$ → P1 以外の因数は 431

(3) $11\theta+a_3, \theta+b_3$ の Q4 での分解

(a) $|a_3|\leq 32$ のとき $11\theta+a_3$ が Q3 分解でき、$11M_3+a_3$ が P1 で分解できないもの

$11\theta-31$ → P1 以外の因数は 283

$11\theta-29$ → P1 以外の因数は 5849

$11\theta-26$ → P1 以外の因数は 11699

$11\theta-22$ → P1 以外の因数は 3191

$11\theta-15$ → P1 以外の因数は 131

$11\theta+6$ → P1 以外の因数は 35129

$11\theta+11$ → P1 以外の因数は 1597

$11\theta+18$ → P1 以外の因数は 35141

(b) $|b_3|\leq 12$ のとき $\theta+b_3$ が Q3 分解でき、M_3+b_3 が P1 で分解できないもの

$\theta-9$ → P1 以外の因数は 199

$\theta-4$ → P1 以外の因数は 1063

$\theta-2$ → P1 以外の因数は 3191

$\theta+1$ → P1 以外の因数は 1597

(4) $13\theta+a_4, \theta+b_4$ の Q4 での分解

(a) $|a_4|\leq 42$ のとき $13\theta+a_4$ が Q4 分解でき、$13M_4+a_4$ が P1 で分解できないもの

該当なし。

(b) $|b_4| \leq 12$ のとき $\theta + b_4$ が Q4 分解でき、$M_4 + b_4$ が P1 で分解できないもの

$\theta - 3$ → P1 以外の因数は 1693

$\theta + 3$ → P1 以外の因数は 1699

$\theta + 10$ → P1 以外の因数は 853

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 34 個となる。

P2 = { 131, 149, 151, 167, 179, 193, 199, 227, 283, 331, 431, 509, 557, 769, 773, 853, 1063, 1151, 1289, 1597, 1693, 1699, 2311, 2699, 3191, 5849, 8081, 8087, 8101, 9649, 11699, 16189, 35129, 35141 }

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 65 個となる。

P = { -1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 131, 149, 151, 167, 179, 193, 199, 227, 283, 331, 431, 509, 557, 769, 773, 853, 1063, 1151, 1289, 1597, 1693, 1699, 2311, 2699, 3191, 5849, 8081, 8087, 8101, 9649, 11699, 16189, 35129, 35141 }

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 $7x + a_1$ 及び $x + b_1$ (M_1=2311)

項番	$7x + a_1$	値($7M_1+a_1$)	$7M_1+a_1$ の P での分解
1	7x − 24	16153	29· 557
2	7x − 20	16157	107· 151
3	7x − 18	16159	11· 13· 113
4	7x − 17	16160	2^5· 5· 101
5	7x − 15	16162	2· 8081
6	7x − 12	16165	5· 53· 61
7	7x − 9	16168	2^3· 43· 47
8	7x − 8	16169	19· 23· 37
9	7x − 7	16170	2· 3· 5· 7^2· 11
10	7x − 3	16174	2· 8087

11	7x	16177	$7\cdot 2311$
12	7x + 5	16182	$2\cdot 3^2\cdot 29\cdot 31$
13	7x + 7	16184	$2^3\cdot 7\cdot 17^2$
14	7x + 8	16185	$3\cdot 5\cdot 13\cdot 83$
15	7x + 11	16188	$2^2\cdot 3\cdot 19\cdot 71$
16	7x + 12	16189	16189
17	7x + 15	16192	$2^6\cdot 11\cdot 23$
18	7x + 17	16194	$2\cdot 3\cdot 2699$
19	7x + 18	16195	$5\cdot 41\cdot 79$
20	7x + 21	16198	$2\cdot 7\cdot 13\cdot 89$
21	7x + 23	16200	$2^3\cdot 3^4\cdot 5^2$
22	7x + 25	16202	$2\cdot 8101$
項番	$x + b_1$	値(M_1+b_1)	M_1+b_1 の P での分解
1	x − 12	2299	$11^2\cdot 19$
2	x − 11	2300	$2^2\cdot 5^2\cdot 23$
3	x − 10	2301	$3\cdot 13\cdot 59$
4	x − 9	2302	$2\cdot 1151$
5	x − 8	2303	$7^2\cdot 47$
6	x − 7	2304	$2^8\cdot 3^2$
7	x − 4	2307	$3\cdot 769$
8	x − 1	2310	$2\cdot 3\cdot 5\cdot 7\cdot 11$
9	x	2311	2311
10	x + 1	2312	$2^3\cdot 17^2$
11	x + 3	2314	$2\cdot 13\cdot 89$
12	x + 6	2317	$7\cdot 331$
13	x + 7	2318	$2\cdot 19\cdot 61$
14	x + 9	2320	$2^4\cdot 5\cdot 29$
15	x + 11	2322	$2\cdot 3^3\cdot 43$
16	x + 12	2323	$23\cdot 101$

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 $5x+a_2$ 及び $2x+b_2$ (M_2=1933)

項番	$5x + a_2$	値($5M_2+a_2$)	$5M_2+a_2$ の P での分解
1	5x − 19	9646	$2\cdot 7\cdot 13\cdot 53$
2	5x − 17	9648	$2^4\cdot 3^2\cdot 67$
3	5x − 16	9649	9649
4	5x − 15	9650	$2\cdot 5^2\cdot 193$
5	5x − 9	9656	$2^3\cdot 17\cdot 71$

6	5x − 8	9657	$3^2 \cdot 29 \cdot 37$
7	5x − 5	9660	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 23$
8	5x − 1	9664	$2^6 \cdot 151$
9	5x + 1	9666	$2^3 \cdot 3 \cdot 179$
10	5x + 6	9671	$19 \cdot 509$
11	5x + 7	9672	$2^3 \cdot 3 \cdot 13 \cdot 31$
12	5x + 10	9675	$3^2 \cdot 5^2 \cdot 43$
13	5x + 11	9676	$2^2 \cdot 41 \cdot 59$
14	5x + 15	9680	$2^4 \cdot 5 \cdot 11^2$
15	5x + 17	9682	$2 \cdot 47 \cdot 103$
16	5x + 20	9685	$5 \cdot 13 \cdot 149$
17	5x + 21	9686	$2 \cdot 29 \cdot 167$
項番	$2x + b_2$	値($2M_2+b_2$)	$2M_2+b_2$ の P での分解
1	2x − 16	3850	$2 \cdot 5^2 \cdot 7 \cdot 11$
2	2x − 14	3852	$2^2 \cdot 3^2 \cdot 107$
3	2x − 12	3854	$2 \cdot 41 \cdot 47$
4	2x − 9	3857	$7 \cdot 19 \cdot 29$
5	2x − 7	3859	$17 \cdot 227$
6	2x − 6	3860	$2^2 \cdot 5 \cdot 193$
7	2x − 5	3861	$3^3 \cdot 11 \cdot 13$
8	2x − 2	3864	$2^3 \cdot 3 \cdot 7 \cdot 23$
9	2x − 1	3865	$5 \cdot 773$
10	2x + 1	3867	$3 \cdot 1289$
11	2x + 3	3869	$53 \cdot 73$
12	2x + 4	3870	$2 \cdot 3^2 \cdot 5 \cdot 43$
13	2x + 5	3871	$7^2 \cdot 79$
14	2x + 6	3872	$2^5 \cdot 11^2$
15	2x + 8	3874	$2 \cdot 13 \cdot 149$
16	2x + 9	3875	$5^3 \cdot 31$
17	2x + 10	3876	$2^2 \cdot 3 \cdot 17 \cdot 19$
18	2x + 13	3879	$3^2 \cdot 431$
19	2x + 14	3880	$2^3 \cdot 5 \cdot 97$

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 $11x + a_3$ 及び $x + b_3$ (M_3=3193)

項番	$11x + a_3$	値($11M_3+a_3$)	$11M_3+a_3$ の P での分解
1	11x − 32	35091	$3^2 \cdot 7 \cdot 557$
2	11x − 31	35092	$2^2 \cdot 31 \cdot 283$

3	$11x-29$	35094	$2\cdot 3\cdot 5849$
4	$11x-27$	35096	$2^3\cdot 41\cdot 107$
5	$11x-26$	35097	$3\cdot 11699$
6	$11x-25$	35098	$2\cdot 7\cdot 23\cdot 109$
7	$11x-22$	35101	$11\cdot 3191$
8	$11x-18$	35105	$5\cdot 7\cdot 17\cdot 59$
9	$11x-15$	35108	$2^2\cdot 67\cdot 131$
10	$11x-14$	35109	$3^2\cdot 47\cdot 83$
11	$11x-11$	35112	$2^3\cdot 3\cdot 7\cdot 11\cdot 19$
12	$11x-10$	35113	$13\cdot 37\cdot 73$
13	$11x-2$	35121	$3\cdot 23\cdot 509$
14	$11x$	35123	$11\cdot 31\cdot 103$
15	$11x+3$	35126	$2\cdot 7\cdot 13\cdot 193$
16	$11x+6$	35129	35129
17	$11x+8$	35131	$19\cdot 43^2$
18	$11x+11$	35134	$2\cdot 11\cdot 1597$
19	$11x+13$	35136	$2^6\cdot 3^2\cdot 61$
20	$11x+16$	35139	$3\cdot 13\cdot 17\cdot 53$
21	$11x+18$	35141	35141
22	$11x+22$	35145	$3^2\cdot 5\cdot 11\cdot 71$
23	$11x+25$	35148	$2^2\cdot 3\cdot 29\cdot 101$
24	$11x+27$	35150	$2\cdot 5^2\cdot 19\cdot 37$
25	$11x+29$	35152	$2^4\cdot 13^3$
26	$11x+31$	35154	$2\cdot 3^4\cdot 7\cdot 31$
27	$11x+32$	35155	$5\cdot 79\cdot 89$
項番	$x+b_3$	値(M_3+b_3)	M_3+b_3 の P での分解
1	$x-11$	3182	$2\cdot 37\cdot 43$
2	$x-9$	3184	$2^4\cdot 199$
3	$x-8$	3185	$5\cdot 7^2\cdot 13$
4	$x-7$	3186	$2\cdot 3^3\cdot 59$
5	$x-4$	3189	$3\cdot 1063$
6	$x-3$	3190	$2\cdot 5\cdot 11\cdot 29$
7	$x-2$	3191	3191
8	$x-1$	3192	$2^3\cdot 3\cdot 7\cdot 19$
9	x	3193	$31\cdot 103$
10	$x+1$	3194	$2\cdot 1597$
11	$x+2$	3195	$3^2\cdot 5\cdot 71$
12	$x+3$	3196	$2^2\cdot 17\cdot 47$
13	$x+5$	3198	$2\cdot 3\cdot 13\cdot 41$

14	x + 7	3200	$2^7 \cdot 5^2$
15	x + 8	3201	$3 \cdot 11 \cdot 97$
16	x + 11	3204	$2^2 \cdot 3^2 \cdot 89$

4.4 $f_4(x)$ に対する 1 次式

$f_4(x)$ に対するふるいに使用する 1 次式は表 4 のようになる。

表 4. ふるいに使用する $13x + a_4$ 及び $x + b_4$ (M_4=1696)

項番	$13x + a_4$	値($13M_4+a_4$)	$13M_4+a_4$ の P での分解
1	13x − 40	22008	$2^3 \cdot 3 \cdot 7 \cdot 131$
2	13x − 38	22010	$2 \cdot 5 \cdot 31 \cdot 71$
3	13x − 37	22011	$3 \cdot 11 \cdot 23 \cdot 29$
4	13x − 33	22015	$5 \cdot 7 \cdot 17 \cdot 37$
5	13x − 32	22016	$2^9 \cdot 43$
6	13x − 31	22017	$3 \cdot 41 \cdot 179$
7	13x − 30	22018	$2 \cdot 101 \cdot 109$
8	13x − 29	22019	$97 \cdot 227$
9	13x − 27	22021	$19^2 \cdot 61$
10	13x − 26	22022	$2 \cdot 7 \cdot 11^2 \cdot 13$
11	13x − 16	22032	$2^4 \cdot 3^4 \cdot 17$
12	13x − 13	22035	$3 \cdot 5 \cdot 13 \cdot 113$
13	13x − 8	22040	$2^3 \cdot 5 \cdot 19 \cdot 29$
14	13x − 7	22041	$3^2 \cdot 31 \cdot 79$
15	13x − 6	22042	$2 \cdot 103 \cdot 107$
16	13x − 5	22043	$7 \cdot 47 \cdot 67$
17	13x − 4	22044	$2^2 \cdot 3 \cdot 11 \cdot 167$
18	13x − 2	22046	$2 \cdot 73 \cdot 151$
19	13x	22048	$2^5 \cdot 13 \cdot 53$
20	13x + 2	22050	$2 \cdot 3^2 \cdot 5^2 \cdot 7^2$
21	13x + 4	22052	$2^2 \cdot 37 \cdot 149$
22	13x + 11	22059	$3^3 \cdot 19 \cdot 43$
23	13x + 24	22072	$2^3 \cdot 31 \cdot 89$
24	13x + 26	22074	$2 \cdot 3 \cdot 13 \cdot 283$
25	13x + 30	22078	$2 \cdot 7 \cdot 19 \cdot 83$
26	13x + 32	22080	$2^6 \cdot 3 \cdot 5 \cdot 23$
27	13x + 41	22089	$3 \cdot 37 \cdot 199$
28	13x + 42	22090	$2 \cdot 5 \cdot 47^2$
項番	$x + b_4$	値(M_4+b_4)	M_4+b_4 の P での分解
1	x − 6	1690	$2 \cdot 5 \cdot 13^2$
2	x − 5	1691	$19 \cdot 89$

3	x − 4	1692	$2^2 \cdot 3^2 \cdot 47$
4	x − 3	1693	1693
5	x − 2	1694	$2 \cdot 7 \cdot 11^2$
6	x − 1	1695	$3 \cdot 5 \cdot 113$
7	x	1696	$2^5 \cdot 53$
8	x + 2	1698	$2 \cdot 3 \cdot 283$
9	x + 3	1699	1699
10	x + 4	1700	$2^2 \cdot 5^2 \cdot 17$
11	x + 5	1701	$3^5 \cdot 7$
12	x + 6	1702	$2 \cdot 23 \cdot 37$
13	x + 7	1703	$13 \cdot 131$
14	x + 8	1704	$2^3 \cdot 3 \cdot 71$
15	x + 9	1705	$5 \cdot 11 \cdot 31$
16	x + 10	1706	$2 \cdot 853$
17	x + 12	1708	$2^2 \cdot 7 \cdot 61$

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、$s_k \le 3$ となるものだけ採用する。
ふるいは S_k が $0,\pm1,\pm2,\cdots$ 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

$S_1 = 0,\pm1,\pm2,\cdots,\pm20$ となる順におこなったふるい結果を表 5 に示す。
ただし、10 以上は $\pm12,\pm14,\pm15,\pm18,\pm20$ だけに限定して実行する。これは、素イデアルの素数対応 2,3,5,7 の倍数から選定する。
ここで、表 5 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。

$$S_1 x + T_1 = (7x + a_1) \cdot (x + b_1) - f_1(x)$$

$$S_1 = a_1 + 7b_1 + 3,\ T_1 = a_1 b_1 - 180$$

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

表 5. $f_1(x)$ 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	25	-4	-1	0	280
2	0	-3	0	-1	0	180
3	0	-24	3	-1	0	252
4	1	5	-1	1	1	-185
5	1	-9	1	1	1	-189

6	2	-8	1	2	1	-94
7	-2	23	-4	-2	1	136
8	-2	-12	1	-2	1	96
9	3	7	-1	1	3	-187
10	3	0	0	3	1	-60
11	-3	22	-4	-1	3	268
12	4	8	-1	4	1	-47
13	4	-20	3	4	1	-60
14	-4	21	-4	-4	1	66
15	-4	0	-1	-4	1	45
16	-5	-8	0	-5	1	36
17	-5	-15	1	-5	1	39
18	6	-18	3	6	1	-39
19	-6	-9	0	-6	1	30
20	7	-17	3	7	1	-33
21	-7	18	-4	-7	1	36
22	8	12	-1	8	1	-24
23	8	5	0	4	2	-45
24	-8	17	-4	-8	1	31
25	9	-15	3	9	1	-25
26	-9	-12	0	-9	1	20
27	10	7	0	10	1	-18
28	-10	15	-4	-10	1	24
29	-10	-20	1	-10	1	20
30	12	-12	3	12	1	-18
31	-12	-8	-1	-4	3	43
32	-12	-15	0	-12	1	15
33	-14	11	-4	-14	1	16
34	15	12	0	15	1	-12
35	15	5	1	5	3	-35
36	-15	-18	0	-15	1	12
37	18	15	0	18	1	-10
38	20	17	0	20	1	-9
39	20	-18	5	10	2	-27

5.2 $f_2(x)$ に対するふるい

$S_2 = 0,\pm1,\pm2,\pm3,\pm4,\pm5,\pm6,\pm8,\pm10,\pm12,\pm15,\pm20$ 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 $S_2, a_2, b_2, G_2, s_2, t_2$ は下記の式中の記号に対応する。

$$S_2 x + T_2 = (5x + a_2)\cdot(2x + b_2) - f_2(x)$$

$$S_2 = 2a_2 + 5b_2 - 7,\ T_2 = a_2 b_2 + 127$$

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

表 6. $f_2(x)$ における DBPS6 のふるい結果

番号	S_2	a_2	b_2	G_2	s_2	t_2
1	0	21	-7	-1	0	20
2	0	6	-1	1	0	121
3	0	1	1	1	0	128
4	0	-9	5	1	0	82
5	0	-19	9	-1	0	44
6	1	-16	8	1	1	-1
7	-1	-17	8	-1	1	9
8	2	17	-5	2	1	21
9	2	7	-1	2	1	60
10	2	-8	5	1	2	87
11	-2	20	-7	-1	2	13
12	-2	15	-5	-2	1	-26
13	-2	-5	3	-2	1	-56
14	3	10	-2	1	3	107
15	-3	17	-6	-1	3	-25
16	-3	7	-2	-1	3	-113
17	-3	-8	4	-1	3	-95
18	4	-17	9	2	2	-13
19	-4	-1	1	-2	2	-63
20	5	11	-2	5	1	21
21	-5	6	-2	-5	1	-23
22	-5	-19	8	-5	1	5
23	6	-1	3	2	3	62
24	8	-15	9	8	1	-1
25	-8	17	-7	-8	1	-1
26	10	1	3	10	1	13
27	-10	-9	3	-10	1	-10
28	-12	-15	5	-4	3	-13
29	15	-9	8	5	3	11
30	-15	1	-2	-5	3	-25
31	20	-19	13	20	1	-6

5.3 $f_3(x)$ に対するふるい

$S_3 = 0,\pm1,\pm2,\pm3,\pm4,\pm5,\pm6,\pm7,\pm9,\pm10,\pm14,\pm15,\pm18$ となる順におこなったふるい結果を表 7 に示す。

ここで、表 7 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。

$$S_3 x + T_3 = (11x + a_3)\cdot(x + b_3) - f_3(x)$$

$$S_3 = a_3 + 11b_3 + 4,\ T_3 = a_3 b_3 + 85$$

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

表 7. $f_3(x)$ 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	29	-3	-1	0	2
2	0	18	-2	1	0	49
3	0	-15	1	1	0	70
4	0	-26	2	1	0	33
5	1	8	-1	1	1	77
6	1	-14	1	1	1	71
7	1	-25	2	1	1	35
8	-1	6	-1	-1	1	-79
9	-1	-27	2	-1	1	-31
10	2	31	-3	2	1	-4
11	2	-2	0	1	2	85
12	-2	27	-3	-2	1	-2
13	-2	16	-2	-1	2	-53
14	3	32	-3	1	3	-11
15	3	-23	2	3	1	13
16	-3	-18	1	-1	3	-67
17	-3	-29	2	-3	1	-9
18	4	11	-1	2	2	37
19	-4	25	-3	-2	2	-5
20	-4	3	-1	-2	2	-41
21	5	-10	1	5	1	15
22	6	13	-1	6	1	12
23	6	-31	3	2	3	-4
24	-6	-32	2	-3	2	-7
25	7	25	-2	7	1	5
26	-7	11	-2	-7	1	-9
27	9	16	-1	3	3	23
28	-9	31	-4	-3	3	13
29	-9	-2	-1	-3	3	-29
30	10	6	0	5	2	17
31	-10	-14	0	-5	2	-17
32	-10	-25	1	-10	1	-6
33	14	32	-2	7	2	3
34	-14	-29	1	-14	1	-4
35	15	11	0	5	3	17
36	-15	25	-4	-15	1	1
37	18	25	-1	6	3	10
38	-18	-11	-1	-6	3	-16

5.4 $f_4(x)$に対するふるい

$S_4 = 0,\pm1,\pm2,\pm3,\pm4,\pm5,\pm6,\pm7,\pm8,\pm9,\pm12,\pm14,\pm15,\pm18,\pm21$となる順におこなったふるい結果を表 8 に示す。

ここで、表 8 中の$S_4, a_4, b_4, G_4, s_4, t_4$は下記の式中の記号に対応する。

$S_4 x + T_4 = (13x + a_4) \cdot (x + b_4) - f_4(x)$

$S_4 = a_4 + 13b_4 + 9,\ T_4 = a_4 b_4 - 150$

$G_4 = sign(S_4) \cdot GCD(|S_4|, |T_4|),\ s_4 = S_4 / G_4,\ t_4 = T_4 / G_4$

表 8. $f_4(x)$における DBPS2 のふるい結果

番号	S_4	a_4	b_4	G_4	s_4	t_4
1	0	30	-3	-1	0	240
2	0	4	-1	-1	0	154
3	1	18	-2	1	1	-186
4	1	-8	0	1	1	-150
5	-1	42	-4	-1	1	318
6	2	32	-3	2	1	-123
7	2	-7	0	2	1	-75
8	2	-33	2	2	1	-108
9	-2	41	-4	-2	1	157
10	-2	2	-1	-2	1	76
11	-2	-37	2	-2	1	112
12	3	-6	0	3	1	-50
13	3	-32	2	1	3	-214
14	-3	-38	2	-1	3	226
15	4	-5	0	2	2	-75
16	4	-31	2	4	1	-53
17	-4	39	-4	-2	2	153
18	-4	26	-3	-4	1	57
19	-4	0	-1	-2	2	75
20	5	-4	0	5	1	-30
21	5	-30	2	5	1	-42
22	-5	-40	2	-5	1	46
23	6	-29	2	2	3	-104
24	-6	24	-3	-6	1	37
25	-6	11	-2	-2	3	86
26	-6	-2	-1	-2	3	74
27	7	11	-1	7	1	-23
28	8	-27	2	4	2	-51
29	9	39	-3	3	3	-89
30	9	0	0	3	3	-50
31	12	42	-3	12	1	-23
32	-12	18	-3	-12	1	17
33	14	18	-1	14	1	-12
34	-15	41	-5	-5	3	71
35	18	-30	3	6	3	-40
36	-18	-27	0	-6	3	25
37	20	11	0	10	2	-15
38	-20	-29	0	-10	2	15
39	21	-27	3	21	1	-11

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(これは通常発生しない)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。$f_4(x)$ は重複チェックの対象が存在しない。

6.1 $f_1(x)$ に対する重複データの削除

$s_1 \le 3$ なので表 12 から $s_1 x + t_1$ が表 12 の $x_1 + b_1$ と一致するもの(区分が 3)を求めると、表 9 が得られる。

表 9. $f_1(x)$ のふるい結果で $s_1 x + t_1$ が $x_1 + b_1$ と一致するもの

No.	a_1	b_1	G_1	s_1	t_1
1	12	0	15	1	-12
2	15	0	18	1	-10
3	17	0	20	1	-9
4	-18	0	-15	1	12

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。

6.2 $f_2(x)$ に対する重複データの削除

$s_2 \le 3$ なので表 13 から $s_2 x + t_2$ が表 13 の $2x_2 + b_2\,(x_2 + b_2/2)$ と一致するもの(区分が 3)を求めると、表 10 が得られる。

表 10. $f_2(x)$ のふるい結果で $s_2 x + t_2$ が $2x_2 + b_2$ と一致するもの

No.	a_2	b_2	G_2	s_2	t_2
1	-19	13	20	1	-6
2	17	-7	-8	1	-1
3	-16	8	1	1	-1
4	-15	9	8	1	-1
5	-19	8	-5	1	5
6	20	-7	-1	2	13

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。

6.3 $f_3(x)$ に対する重複データの削除

$s_3 \le 3$ なので表 14 から $s_3 x + t_3$ が表 14 の $x_3 + b_3$ と一致するもの(区分が 3)を求めると、表 11 が得られる。

表 11. $f_3(x)$のふるい結果でs_3x+t_3がx_3+b_3と一致するもの

No.	a_3	b_3	G_3	s_3	t_3
1	11	-2	-7	1	-9
2	-29	2	-3	1	-9
3	-29	1	-14	1	-4
4	31	-3	2	1	-4
5	27	-3	-2	1	-2
6	25	-4	-15	1	1
7	25	-2	7	1	5

No.3 と No.6 の乗算で互いのs_3x+t_3がx_3+b_3が一致し、別の結果$(11x-29)(25x-4)=210$となるため、No.6 を重複削除する。

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 及び-1 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。
2 の区分のものは、s_1x+t_1が共通のため 2 個の等式をs_1x+t_1を使用して結合して、行列を作成するためs_1x+t_1の因数分解は不要である。

7.1 $f_1(x)$に対するふるいデータの選定

表 12 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 12. $f_1(x)$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	-3	0	-1	0	180	1	180	$2^2\cdot 3^2\cdot 5$
2	-24	3	-1	0	252	1	252	$2^2\cdot 3^2\cdot 7$
3	25	-4	-1	0	280	1	280	$2^3\cdot 5\cdot 7$
---	-9	1	1	1	-189	0	2122	-----
4	5	-1	1	1	-185	1	2126	$2\cdot 1063$
---	-8	1	2	1	-94	0	2217	-----
5	0	0	3	1	-60	2	2251	-----
5	-20	3	4	1	-60	2	2251	-----

6	8	-1	4	1	-47	1	2264	$2^4 \cdot 283$
7	-18	3	6	1	-39	1	2272	$2^5 \cdot 71$
8	-17	3	7	1	-33	1	2278	$2 \cdot 17 \cdot 67$
---	-15	3	9	1	-25	0	2286	-----
---	12	-1	8	1	-24	0	2287	-----
9	7	0	10	1	-18	2	2293	-----
9	-12	3	12	1	-18	2	2293	-----
19	12	0	15	1	-12	3	2299	$11^2 \cdot 19$
20	15	0	18	1	-10	3	2301	$3 \cdot 13 \cdot 59$
21	17	0	20	1	-9	3	2302	$2 \cdot 1151$
22	-18	0	-15	1	12	3	2323	$23 \cdot 101$
---	-15	0	-12	1	15	0	2326	-----
10	11	-4	-14	1	16	1	2327	$13 \cdot 179$
11	-20	1	-10	1	20	1	2331	$3^2 \cdot 7 \cdot 37$
12	-12	0	-9	1	20	1	2331	$3^2 \cdot 7 \cdot 37$
---	15	-4	-10	1	24	0	2335	-----
---	-9	0	-6	1	30	0	2341	-----
---	17	-4	-8	1	31	0	2342	-----
13	18	-4	-7	1	36	2	2347	-----
13	-8	0	-5	1	36	2	2347	-----
14	-15	1	-5	1	39	1	2350	$2 \cdot 5^2 \cdot 47$
15	0	-1	-4	1	45	1	2356	$2^2 \cdot 19 \cdot 31$
---	21	-4	-4	1	66	0	2377	-----
16	-12	1	-2	1	96	1	2407	$29 \cdot 83$
---	23	-4	-2	1	136	0	2447	-----
17	5	0	4	2	-45	1	4577	$23 \cdot 199$
---	-18	5	10	2	-27	0	4595	-----
---	7	-1	1	3	-187	0	6746	-----
---	5	1	5	3	-35	0	6898	-----
18	-8	-1	-4	3	43	1	6976	$26 \cdot 109$
---	22	-4	-1	3	268	0	7201	-----

7.2 $f_2(x)$ に対するふるいデータの選定

表 13 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 1,2 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 13. $f_2(x)$ 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
23	21	-7	-1	0	20	1	20	$2^2 \cdot 5$
24	-19	9	-1	0	44	1	44	$2^2 \cdot 11$
25	-9	5	1	0	82	1	82	$2 \cdot 41$
26	6	-1	1	0	121	1	121	11^2
27	1	1	1	0	128	1	128	2^7
---	-5	3	-2	1	-56	0	1877	-----

---	15	-5	-2	1	-26	0	1907	-----
---	6	-2	-5	1	-23	0	1910	-----
---	-9	3	-10	1	-10	0	1923	-----
33	-19	13	20	1	-6	3	1927	41· 47
34	17	-7	-8	1	-1	3	1932	2^2· 3· 7· 23
35	-16	8	1	1	-1	3	1932	2^2· 3· 7· 23
36	-15	9	8	1	-1	3	1932	2^2· 3· 7· 23
37	-19	8	-5	1	5	3	1938	2· 3· 17· 19
---	-17	8	-1	1	9	0	1942	-----
---	1	3	10	1	13	0	1946	-----
28	17	-5	2	1	21	2	1954	-----
28	11	-2	5	1	21	2	1954	-----
---	7	-1	2	1	60	0	1993	-----
---	-1	1	-2	2	-63	0	3803	-----
---	-17	9	2	2	-13	0	3853	-----
38	20	-7	-1	2	13	3	3879	3^2· 431
29	-8	5	1	2	87	1	3953	59· 67
---	7	-2	-1	3	-113	0	5686	-----
30	-8	4	-1	3	-95	1	5704	2^3· 23· 31
31	1	-2	-5	3	-25	2	5774	-----
31	17	-6	-1	3	-25	2	5774	-----
---	-15	5	-4	3	-13	0	5786	-----
32	-9	8	5	3	11	1	5810	2· 5· 7· 83
---	-1	3	2	3	62	0	5861	-----
---	10	-2	1	3	107	0	5906	-----

7.3 $f_3(x)$に対するふるいデータの選定

表 14 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 1,2 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。区分が-1 のデータは選択する前に重複削除されたものである。

表 14. $f_3(x)$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
39	29	-3	-1	0	2	1	2	2
40	-26	2	1	0	33	1	33	3· 11
41	18	-2	1	0	49	1	49	7^2
42	-15	1	1	0	70	1	70	2· 5· 7
---	6	-1	-1	1	-79	0	3114	-----
43	-27	2	-1	1	-31	1	3162	2· 3· 17· 31
52	11	-2	-7	1	-9	3	3184	2· 4· 199
53	-29	2	-3	1	-9	3	3184	2· 4· 199
---	-25	1	-10	1	-6	0	3187	-----
54	-29	1	-14	1	-4	3	3189	3· 1063

55	31	-3	2	1	-4	3	3189	3· 1063
56	27	-3	-2	1	-2	3	3191	3191
---	25	-4	-15	1	1	-1	3194	重複削除
57	25	-2	7	1	5	3	3198	2· 1597
---	13	-1	6	1	12	0	3205	-----
---	-23	2	3	1	13	0	3206	-----
---	-10	1	5	1	15	0	3208	-----
---	-25	2	1	1	35	0	3228	-----
44	-14	1	1	1	71	1	3264	2^6· 3· 17
45	8	-1	1	1	77	1	3270	2· 3· 5· 109
---	16	-2	-1	2	-53	0	6333	-----
46	3	-1	-2	2	-41	1	6345	3^3· 5· 47
47	-14	0	-5	2	-17	1	6369	3· 11· 193
---	-32	2	-3	2	-7	0	6379	-----
---	25	-3	-2	2	-5	0	6381	-----
---	32	-2	7	2	3	0	6389	-----
---	6	0	5	2	17	0	6403	-----
---	11	-1	2	2	37	0	6423	-----
---	-2	0	1	2	85	0	6471	-----
48	-18	1	-1	3	-67	1	9512	2^3· 29· 41
---	-2	-1	-3	3	-29	0	9550	-----
49	-11	-1	-6	3	-16	1	9563	73· 131
50	32	-3	1	3	-11	1	9568	2^5· 13· 23
---	-31	3	2	3	-4	0	9575	-----
---	25	-1	6	3	10	0	9589	-----
51	31	-4	-3	3	13	1	9592	2^3· 11· 109
---	11	0	5	3	17	0	9596	-----
---	16	-1	3	3	23	0	9602	-----

7.4 $f_4(x)$に対するふるいデータの選定

表 15 に $f_4(x)$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 15. $f_4(x)$ に対するふるいデータからの選定結果

No.	a_4	b_4	G_4	s_4	t_4	区分	$s_4M_4+t_4$	
							値	P の分解
58	4	-1	-1	0	154	1	154	2· 7· 11
59	30	-3	-1	0	240	1	240	2^4· 3· 5
60	18	-2	1	1	-186	1	1510	2· 5· 151
61	-8	0	1	1	-150	1	1546	2· 773
62	32	-3	2	1	-123	1	1573	11^2· 13
---	-33	2	2	1	-108	0	1588	-----
---	-7	0	2	1	-75	0	1621	-----
63	-31	2	4	1	-53	1	1643	31· 53
---	-6	0	3	1	-50	0	1646	-----

---	-30	2	5	1	-42	0	1654	-----
64	-4	0	5	1	-30	1	1666	$2\cdot 7^2\cdot 17$
65	11	-1	7	1	-23	2	1673	-----
65	42	-3	12	1	-23	2	1673	-----
---	18	-1	14	1	-12	0	1684	-----
---	-27	3	21	1	-11	0	1685	-----
---	18	-3	-12	1	17	0	1713	-----
---	24	-3	-6	1	37	0	1733	-----
66	-40	2	-5	1	46	1	1742	$2\cdot 13\cdot 67$
---	26	-3	-4	1	57	0	1753	-----
---	2	-1	-2	1	76	0	1772	-----
67	-37	2	-2	1	112	1	1808	$2^4\cdot 113$
68	41	-4	-2	1	157	1	1853	$17\cdot 109$
69	42	-4	-1	1	318	1	2014	$2\cdot 19\cdot 53$
70	-5	0	2	2	-75	1	3317	$31\cdot 107$
---	-27	2	4	2	-51	0	3341	-----
---	11	0	10	2	-15	0	3377	-----
---	-29	0	-10	2	15	0	3407	-----
---	0	-1	-2	2	75	0	3467	-----
---	39	-4	-2	2	153	0	3545	-----
---	-32	2	1	3	-214	0	4874	-----
71	-29	2	2	3	-104	1	4984	$2^3\cdot 7\cdot 89$
---	39	-3	3	3	-89	0	4999	-----
---	0	0	3	3	-50	0	5038	-----
---	-30	3	6	3	-40	0	5048	-----
---	-27	0	-6	3	25	0	5113	-----
72	41	-5	-5	3	71	1	5159	$7\cdot 11\cdot 67$
73	-2	-1	-2	3	74	1	5162	$2\cdot 29\cdot 89$
74	11	-2	-2	3	86	1	5174	$2\cdot 13\cdot 199$
---	-38	2	-1	3	226	0	5314	-----

8. 行列作成

8.1 ふるい結果による行列作成

表 12,表 13,表 14,表 15 の選定されたデータに対して、表 1,表 2,表 3,表 4 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 74×65 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 12 の No.2 のデータは$(7M_1-24)\cdot(M_1+3)\equiv -2^2\cdot 3^2\cdot 7 \pmod{N}$であり、これに$M_1=2311$を代入すると$16153\cdot 23145\equiv -2^2\cdot 3^2\cdot 7 \pmod{N}$、即ち$2\cdot 13\cdot 29\cdot 89\cdot 557\equiv -2^2\cdot 3^2\cdot 7 \pmod{N}$、即ち$13\cdot 29\cdot 89\cdot 557\equiv -1\cdot 2\cdot 3^2\cdot 7 \pmod{N}$となる。素数基底 P の k 番目の素数を p_k とすると、p_1=-1、p_2=2、p_3=3、p_5=7、p_7=13、p_{11}=29、p_{25}=89、p_{44}=557 となるため表 16 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 12 の No.5 の 2 つのデータは下記となる。

$$7\cdot M_1^2\equiv 3\cdot(M_1-60) \pmod{N}$$

$$(7M_1-20)\cdot(M_1+3)\equiv 4\cdot(M_1-60) \pmod{N}$$

この両式から(M_1-60)を消去し、$M_1=2311$を代入すると次式が得られる。

$$3\cdot 16157\cdot 2314\equiv 4\cdot 7\cdot 2311^2 \pmod{N}$$

これを因数分解すると次式が得られる。

$$3\cdot 13\cdot 89\cdot 107\cdot 151\equiv 2\cdot 7\cdot 2311^2$$

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_7=13、p_{25}=89、p_{29}=107、p_{34}=151、p_{54}=2311 となるため表 16 の No.5 のデータが得られる。

表 16 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 65 番は 35141 に対応する。

表 16. DBPS2 のふるいにより作成された行列

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
1	1	-1	-2	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0
2	1	-1	-2	0	-1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	1	-2	1	-1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
4	0	1	3	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	-1	1	0	-1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0	-2	0	0	0	0	0	0	0	0	0	0	0
6	0	-4	2	2	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	-5	-1	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	5	0	1	-1	0	1	-1	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	-3	-1	2	-1	0	1	-2	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0
10	1	1	2	0	-1	0	-1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	1	2	-2	-1	-1	0	0	2	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	1	0	-4	1	-1	0	0	0	0	0	0	0	-1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
13	0	0	-1	-2	1	0	0	0	1	1	0	0	1	-1	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
14	1	3	0	-3	0	0	0	2	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
15	1	-3	1	1	2	1	0	0	-1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
16	1	2	0	1	0	0	0	2	0	0	-1	0	0	0	0	0	1	0	1	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	-1	2	0	0	0	0	0	0	-1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
18	1	-7	1	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	-1	-1	0	-2	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0
20	0	5	-3	0	0	1	-1	0	0	1	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
21	0	-2	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
22	1	0	-1	-1	0	1	1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
23	1	-1	0	-1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	1	-1	0	3	1	-1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	2	0	0	2	0	0	1	0	0	0	0	0	-1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	1	0	-2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	-6	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	5	-2	-1	1	-1	-1	0	0	1	0	0	0	1	0	-1	0	1	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	2	0	2	0	0	0	0	0	1	0	1	0	0	0	0	-1	0	-1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

30	1-2 4 1 0 0 0 0 0-1 1-1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
31	0-1-4 2-1 0 0 0 0-1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0-1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
32	0 3 0-2-1 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0-1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
33	0-1 2-1 1 0 1 0 0 0 0 0 0-1 0-1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
34	1-4-1 0-1 0 0 1 0-1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
35	0-1-1 0-1 0 1 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0
36	0-4-1 5-1 0 0 0 0-1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
37	1 1-1-1 1 0 2-1-1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
38	1 0-2 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
39	1 4 0 1 0 1 3 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
40	0 0 2 1 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
41	0 0 0 0-2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1
42	0 2 0-1-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
43	1 2 1 1 0 0 0-1 0 0 0-1 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
44	0-5 1 0 0 0 0-1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
45	0 2 0-1 1 0 0 0 2 0 0 0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
46	1 3-2-1 2 0 1 0 1 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
47	1 0 1-1 0-1 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
48	1-2 0 1 1 0 0 1 0 0-1 0 0-1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
49	1 5 1 0 2 1 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
50	0-4 0 2 0 1-1 0 0-1 1 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
51	1-2 4 0 1-1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
52	1-3 0 0-1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0
53	1-3 2 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
54	1 1 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0
55	0 1 3 1 1 1 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
56	1 1 0 3 0 1 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0
57	0 1 0 0-1 0-1 0 0 0 1 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0
58	1 1 1 1-1-1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
59	1-3-1-1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
60	0 1 0-1 1 3 0 1 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
61	0 7 0 1 0 0 0 0 1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
62	0 5 1 1 0-2-1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
63	0-1 2 0 0 0 0 0 0 0 0-1 0 1 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
64	0 6 1-1-2 1 0-1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
65	0-1-5 0 1 0 0 0-1 0 0 0 0 0-1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
66	1 3 2-1 1 0-1 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
67	1-4 2 0 0 1 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
68	1 1 3 0 0 0 0-1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
69	1 2 2 1 0 0 0 0-1 0 0 0 0 0 0 3-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
70	0 4 0 0 1 0 0 0 0 0 0-1 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
71	0-3 1 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
72	1 0 1-1-1-1 0 0 1 0 0 0 1 0 0 0 0 0 0-1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
73	1-1 1 1 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 1 0 0-1 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
74	1-1 3 0 1 2-1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

8.2 行列の縮小

表 16 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 26,41,43,44,47,49,50,53,55 及び 58～65 番目までの 17 個の素数、97,331,509,557,853,1151,1289,1699,2699 及び 8081 以降の素数を除き、これに対応して 12 個の行データを削除する。

従って、素数基底 P は 48 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, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79,

83, 89, 101, 103, 107, 109, 113, 131, 149, 151, 167, 179, 193, 199, 227, 283, 431, 769, 773, 1063, 1597, 1693, 2311, 3191, 5849}

縮小した 62×48 次元の行列を表 17 に示す。

表 17. 縮小した行列

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	0	1	3	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0
2	0	-1	1	0	-1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	-2	0	0
3	0	-4	2	2	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0
4	0	-5	-1	0	0	1	2	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0
5	0	5	0	1	-1	0	1	-1	0	0	0	0	0	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	0	0	0	0	0	0	0	0	0	0
6	0	-3	-1	2	-1	0	1	-2	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0
7	1	1	2	0	-1	0	-1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	1	0	0	0	0	0	0	0
8	1	2	-2	-1	-1	0	0	2	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	1	0	-4	1	-1	0	0	0	0	0	0	0	-1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
10	0	0	-1	-2	1	0	0	0	1	1	0	0	1	-1	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	1	0	0
11	1	-3	1	1	2	1	0	0	-1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
12	1	2	0	1	0	0	0	2	0	0	-1	0	0	0	0	0	1	0	1	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	-1	2	0	0	0	0	0	0	-1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	1	0	0
14	1	-7	1	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	5	-3	0	0	1	-1	0	0	1	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
16	1	0	-1	-1	0	1	1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
17	1	-1	0	-1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
18	1	-1	0	3	1	-1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	2	0	0	2	0	0	1	0	0	0	0	0	-1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	5	-2	-1	1	-1	-1	0	0	1	0	0	0	1	0	-1	0	1	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	2	0	2	0	0	0	0	0	1	0	1	0	0	0	0	-1	0	-1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	1	-2	4	1	0	0	0	0	0	-1	1	-1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	-1	-4	2	-1	0	0	0	0	-1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	-1	1	0	0	0	0	0	0	0	0	0	0	0	0
24	0	3	0	-2	-1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	-1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	-1	2	-1	1	0	1	0	0	0	0	0	0	-1	0	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
26	1	-4	-1	0	-1	0	0	1	0	-1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
27	0	-4	-1	5	-1	0	0	0	0	-1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
28	1	1	-1	-1	1	0	2	-1	-1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	1	0	-2	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	-1	0	0	0	0	0	0	0	0
30	1	4	0	1	0	1	3	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	2	0	-1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
32	1	2	1	1	0	0	0	-1	0	0	0	-1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	-5	1	0	0	0	0	-1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
34	0	2	0	-1	1	0	0	0	2	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	1	3	-2	-1	2	0	1	0	1	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
36	1	0	1	-1	0	-1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0
37	1	-2	0	1	1	0	0	1	0	0	-1	0	0	-1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
38	1	5	1	0	2	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	-4	0	2	0	1	-1	0	0	-1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	1	-2	4	0	1	-1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
41	1	-3	0	0	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	1	0	0	1	0
42	1	-3	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	1
43	1	1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	1	0	0	0	1
44	0	1	3	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0
45	1	1	0	3	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0
46	0	1	0	0	-1	0	-1	0	0	0	1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
47	1	1	1	1	-1	-1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48	1	-3	-1	-1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
49	0	1	0	-1	1	3	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
50	0	7	0	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0

51 0 5 1 1 0-2-1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
52 0-1 2 0 0 0 0 0 0 0 0 0-1 0 1 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0
53 0 6 1-1-2 1 0-1 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
54 0-1-5 0 1 0 0 0-1 0 0 0 0 0 0-1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
55 1 3 2-1 1 0-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
56 1-4 2 0 0 1 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
57 1 1 3 0 0 0 0-1 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0
58 1 2 2 1 0 0 0 0-1 0 0 0 0 0 0 0 3-1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
59 0 4 0 0 1 0 0 0 0 0 0 0-1 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
60 1 0 1-1-1-1-1 0 0 1 0 0 0 1 0 0 0 0 0 0 0-1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
61 1-1 1 1 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0-1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
62 1-1 3 0 1 2-1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0-1 0 0 0 0 0 0 0 0 0 0 0

9. 因数分解

「2 次の DBPS2 による因数分解例 2」を参照。

本結果から 16 個の関係が得られ、その中の 8 個から 18689147=2389×7823 と因数分解され、残り 8 個は自明解で因数分解できない。