2 次の DBPS2 に因数分解例 2

2006/11/09　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、GNFS(一般数体ふるい法)で行う処理は使用しないで、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. ふるい

詳細は「2 次の DBPS2 によるふるい例 2」を参照。

3.1 素数基底(P)

-1 及び 113 までの素数と、イデアル基底を使用して求めた素数基底は下記のように 65 個の素数から構成される。

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 }

3.2 ふるいに使用する 1 次式

$S_k x + T_k = (\alpha_k x + a_k) \cdot (\beta_k + b_k) - f_k(x)$ 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。

(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。

ここで、$|a_1| \leq 25, |b_1| \leq 12$ とする。

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· 2311
12	7x + 5	16182	2· 3^2· 29· 31
13	7x + 7	16184	2^3· 7· 17^2
14	7x + 8	16185	3· 5· 13· 83
15	7x + 11	16188	2^2· 3· 19· 71
16	7x + 12	16189	16189
17	7x + 15	16192	2^6· 11· 23
18	7x + 17	16194	2· 3· 2699
19	7x + 18	16195	5· 41· 79
20	7x + 21	16198	2· 7· 13· 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	$23 \cdot 101$

(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。

ここで、$|a_2| \le 21, |b_2| \le 16$ とする。

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· 47· 103
16	5x + 20	9685	5· 13· 149
17	5x + 21	9686	2· 29· 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· 41· 47
4	2x − 9	3857	7· 19· 29
5	2x − 7	3859	17· 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· 773
10	2x + 1	3867	3· 1289
11	2x + 3	3869	53· 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· 13· 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	$2^3\cdot 5\cdot 97$

(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。

ここで、$|a_3| \le 32, |b_3| \le 12$ とする。

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· 11699
6	11x − 25	35098	2· 7· 23· 109
7	11x − 22	35101	11· 3191
8	11x − 18	35105	5· 7· 17· 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) $f_4(x)$ 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。

これにより、$|a_4| \leq 42, |b_4| \leq 12$ とする。

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	$2^2 \cdot 7 \cdot 61$

3.3 ふるい結果

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 3 章で作成したものを使用し、$s_k \leq 3$ となるものだけ採用する。

(1) $f_1(x)$ に対するふるいデータの選定

表 5 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 5. $f_1(x)$ 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	-----

(2) $f_2(x)$ に対するふるいデータの選定

表 6 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 6. $f_2(x)$ 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	$41\cdot 47$
34	17	-7	-8	1	-1	3	1932	$2^2\cdot 3\cdot 7\cdot 23$
35	-16	8	1	1	-1	3	1932	$2^2\cdot 3\cdot 7\cdot 23$
36	-15	9	8	1	-1	3	1932	$2^2\cdot 3\cdot 7\cdot 23$
37	-19	8	-5	1	5	3	1938	$2\cdot 3\cdot 17\cdot 19$
---	-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	$3^2 \cdot 431$
29	-8	5	1	2	87	1	3953	$59 \cdot 67$
---	7	-2	-1	3	-113	0	5686	-----
30	-8	4	-1	3	-95	1	5704	$2^3 \cdot 23 \cdot 31$
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	$2 \cdot 5 \cdot 7 \cdot 83$
---	-1	3	2	3	62	0	5861	-----
---	10	-2	1	3	107	0	5906	-----

(3) $f_3(x)$に対するふるいデータの選定

表 7 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 7. $f_3(x)$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	$3 \cdot 11$
41	18	-2	1	0	49	1	49	7^2
42	-15	1	1	0	70	1	70	$2 \cdot 5 \cdot 7$
---	6	-1	-1	1	-79	0	3114	-----
43	-27	2	-1	1	-31	1	3162	$2 \cdot 3 \cdot 17 \cdot 31$
52	11	-2	-7	1	-9	3	3184	$2 \cdot 4 \cdot 199$
53	-29	2	-3	1	-9	3	3184	$2 \cdot 4 \cdot 199$
---	-25	1	-10	1	-6	0	3187	-----
54	-29	1	-14	1	-4	3	3189	$3 \cdot 1063$
55	31	-3	2	1	-4	3	3189	$3 \cdot 1063$
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	$2 \cdot 1597$
---	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	$2^6 \cdot 3 \cdot 17$
45	8	-1	1	1	77	1	3270	$2 \cdot 3 \cdot 5 \cdot 109$
---	16	-2	-1	2	-53	0	6333	-----
46	3	-1	-2	2	-41	1	6345	$3^3 \cdot 5 \cdot 47$
47	-14	0	-5	2	-17	1	6369	$3 \cdot 11 \cdot 193$
---	-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	$2^3 \cdot 29 \cdot 41$
---	-2	-1	-3	3	-29	0	9550	-----
49	-11	-1	-6	3	-16	1	9563	$73 \cdot 131$
50	32	-3	1	3	-11	1	9568	$2^5 \cdot 13 \cdot 23$
---	-31	3	2	3	-4	0	9575	-----
---	25	-1	6	3	10	0	9589	-----
51	31	-4	-3	3	13	1	9592	$2^3 \cdot 11 \cdot 109$
---	11	0	5	3	17	0	9596	-----
---	16	-1	3	3	23	0	9602	-----

(4) $f_4(x)$に対するふるいデータの選定

表 8 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 8. $f_4(x)$ 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	$2 \cdot 7 \cdot 11$
59	30	-3	-1	0	240	1	240	$2^4 \cdot 3 \cdot 5$
60	18	-2	1	1	-186	1	1510	$2 \cdot 5 \cdot 151$
61	-8	0	1	1	-150	1	1546	$2 \cdot 773$
62	32	-3	2	1	-123	1	1573	$11^2 \cdot 13$
---	-33	2	2	1	-108	0	1588	-----
---	-7	0	2	1	-75	0	1621	-----
63	-31	2	4	1	-53	1	1643	$31 \cdot 53$
---	-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	-----

3.4 ふるい結果による行列

表 8,9,10,11 から 74×65 次元の行列ができるが、17 個の素数は 1 回しか使用されないため、これを削除すると 62×48 次元の行列が得られる。このとき、素数基底 P は 17 個除き下記の 48 個となり、その順に行列の列に対応する。

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 12 に示す。

表 12. 縮小した行列

```
    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 3 3 3 3 3 3 4 4 4 4 4 4 4 4
    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 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8
 ----------------------------------------------------------------------------------------------------
 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 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 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
 4  0-5-1 0 0 1 2 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
 5  0 5 0 1-1 0 1-1 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 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 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 0-1 0 0
 7  1 1 2 0-1 0-1 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 0 0 0 0 0-1 0 0 0 0 0 1 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 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 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 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 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 0 1 0 0
12  1 2 0 1 0 0 0 2 0 0-1 0 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
13  0-1 2 0 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 0 0 0 0 0 0 0 0 0 0 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 0 0 0 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 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 0-1 0 0 0 1 0 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 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 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 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 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 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 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 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 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 0 1 0 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 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
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 0 0 0 1 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 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 0 0 0 0 0 0 1 0 0 0 0 0 1 0 -1 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 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 1 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 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 0 0 -1 0 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 0 1 0 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 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 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 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
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 0 -1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 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 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 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 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 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 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 0 0 1 0
47	1 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 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 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
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 0 0 -1 0 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 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 -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 1 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 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
54	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 0 0 0 -1 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 -1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 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 -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 -1 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
59	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 -1 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 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 0 1 0 0 0 0 0 0 0 0 0 0 0
61	1 -1 1 1 0 0 0 0 0 0 -1 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
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 -1 0 0 0 0 0 0 0 0 0 0

4. 行列の従属行の計算

(1) 0-1 行列の作成

表 12 の行列の各要素に対して (mod 2) を実施した結果を表 13 に示す。

表 13. 0-1 行列（A）

	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 3 3 3 3 3 3 4 4 4 4 4 4 4 4
	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 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8
1	0 1 1 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 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 0 0 0 0
3	0 0 0 0 1 1 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 1 0 0 0 0 0 0 0 0
4	0 1 1 0 0 1 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
5	0 1 0 1 1 0 1 1 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 0 0 0 0 0 0 0 0 0 0 0 0

```
 6  0 1 1 0 1 0 1 0 0 0 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 1 0 0
 7  1 1 0 0 1 0 1 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 0 1 0 0 0 0 0 0 0
 8  1 0 0 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 1 0 0 0 0 0 0 0 0 0 0 0 0
 9  1 0 0 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 1 0 0
10  0 0 1 0 1 0 0 0 1 1 0 0 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 0 1 0 0 0 0 1 0 0
11  1 1 1 1 0 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 1 0 0
12  1 0 0 1 0 0 0 0 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
13  0 1 0 0 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 1 0 0 0 0 0 0 0 1 0 0
14  1 1 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 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
15  0 1 1 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 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 1 0 0 0 1 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 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0
18  1 1 0 1 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
19  0 0 0 0 0 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
20  0 1 0 1 1 1 1 0 0 1 0 0 0 1 0 1 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
21  0 0 0 0 0 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
22  1 0 0 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
23  0 1 0 0 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
24  0 1 0 0 1 0 1 1 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
25  0 1 0 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 1 0 0 0 0 0 0 0
26  1 0 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
27  0 0 1 1 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
28  1 1 1 1 1 0 0 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 0 0 0 1 0 0 0 0 0 0 0 0 0
29  1 0 0 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 0 0 0 1 0 0 0 0 0 1 0 1 0
30  1 0 0 1 0 1 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 0 0
31  0 0 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 1 0
32  1 0 1 1 0 0 0 1 0 0 0 1 0 1 0 0 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
33  0 1 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 1 0 0
34  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 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
35  1 1 0 1 0 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
36  1 0 1 1 0 1 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 1 0 0 0 0 0 0 0 0 0 0 0
37  1 0 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 1 0 0 0 0 0
38  1 1 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
39  0 0 0 0 0 1 1 0 0 1 1 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
40  1 0 0 0 1 1 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 1 0 0 0 0 0 0 0
41  1 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 0 0 0 1 0 0 0 0 0 0 1 0 0 1 0
42  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 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 1 1 0 0 1
44  0 1 1 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 1 0 0 0 0 0
45  1 1 0 1 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 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 1 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 1 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 1 1 1 1 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 1 0 0 0
49  0 1 0 1 1 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 1 0 0 0 0 0 0 0 0 0 0 0 0 0
50  0 1 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 1 0 0 0 0 0
51  0 1 1 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 1 0 0 0
52  0 1 0 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 1 0 0 0 1 0 0 0 0 0
53  0 0 1 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 1 0 0 0 0 0 0 0 0 0
54  0 1 1 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 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
55  1 1 0 1 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 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0
56  1 0 0 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 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
57  1 1 1 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 1 0 0 0 0 0 0 0 0
58  1 0 0 1 0 0 0 0 1 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
59  0 0 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 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
60  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 1 0 0 0 0 0 0 0 0 0
61  1 1 1 1 0 0 0 0 0 1 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
62  1 1 1 0 1 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 0 0 0 0 0 0 0
```

(2) ガウス消去計算結果

0-1 行列 A の横に単位行列 I を追加した行列 A+I をガウス消去法で A の下三角部分を消去し、A の行が完全に消去された部分に対応する I の部分を表 14 に示す。

表 14.　(A+I)のガウス消去結果(A が完全消去された I の部分)

```
   0000000001111111111222222222233333333334444444444555555555566
   1234567890123456789012345678901234567890123456789012345678901234567890123456789012
---------------------------------------------------------------------------------------------------------------------------
 1 0000100000000001101011000000101001011101000000010000000000000000
 2 0001100000100001011010010011010011101001111010000000000000000000
 3 0101101001100011001010100010010110111010000000001000000000000000
 4 0100010110000000000000000000000000000000000000000000000000000000
 5 0001100000100101001010000010000011101000000000010010000000000000
 6 1000000000000000000000000000000000000000000000010000000000000000
 7 0010101011010100111110011000110000110011111001000001100000000000
 8 1010100000001001000111110001010010100010011000010001010000000000
 9 1000100010010010000010110011011010110010111001000001001000000000
10 0101000110011000010100101111100001111001011000000000100010000000
11 0010001001100000000100001110010001011000101100000000010000100000
12 1111101111110001011110010001000001110011000000000000100000010000
13 0001101001000101011000101111100101000000000000000000000000001000
14 1011000000100001011010100000000001011001100001000001000000000100
15 1011000110010110001110111111011110011111010000000000100000000010
16 0100001111011010010101110011000000000001000000000000000000000001
```

(3)　従属行

表 14 から 16 組の従属関係が発生することが分かる。各組の従属関係は該当する列番号の位置に 1 がある、番号に対応する行番号の組み合わせとなる。従って下記 16 組の従属関係が得られる。

(a) 従属行 1：　5, 15, 16, 18, 20, 21, 28, 30, 33, 35, 36, 37, 39, 47

(b) 従属行 2：　4, 5, 11, 16, 18, 19, 21, 24, 27, 28, 30, 33, 34, 35,37,40,41,42,43,45

(c) 従属行 3：　2, 4, 5, 7, 10, 11, 15, 16, 19, 21, 23, 27, 30, 32, 33, 35, 36,37,39,49

(d) 従属行 4：　2, 6, 8, 9

(e) 従属行 5：　4, 5, 11, 14, 16, 19, 21, 27, 33, 34, 35, 37, 48, 51

(f) 従属行 6：　1, 44

(g) 従属行 7：　3, 5, 7, 9, 10, 12, 14, 17, 18, 19, 20, 21, 24, 25, 29, 30, 35, 36, 39, 40, 41, 42, 43, 46, 52, 53

(h) 従属行 8：　1, 3, 5, 13, 16, 20, 21, 22, 23, 24, 28, 30,33,35, 39,42,43,48,52, 54

(i) 従属行 9：　1, 5, 9, 12, 15, 21, 23,24,27,28,30,31,33,35,36,39,41,42,43,46,52,55

(j) 従属行 10：　2, 4,8,9,12,13,18,20,23,25,26,27,28,29,34,35,36,37,40,42,43,52,56

(k) 従属行 11：　3, 7, 10, 11, 19, 24, 25, 26, 29, 33, 35, 36, 40, 42, 43, 52, 57

(l) 従属行 12：　1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 16, 18, 19, 20, 21, 24, 28, 34, 35, 36, 39, 40, 52, 58

(m)従属行 13：　4, 5, 7, 10, 14, 16, 18, 19, 23, 25, 26, 27, 28, 29, 32, 34, 59

(n) 従属行 14：　1, 3, 4, 11, 16, 18, 19, 21, 23, 34, 36, 37, 40, 41, 46, 52, 60

(o) 従属行 15： 1, 3, 4, 8, 9, 12, 14, 15, 19, 20, 21, 23, 24, 25, 26, 27, 29, 30, 31, 32, 35, 36, 37, 38, 40, 52, 61

(p) 従属行 16： 2, 7, 8, 9, 10, 12, 13, 15, 18, 20, 22, 23, 24, 27, 28, 39, 62

4. 因数分解

(1) 従属行 1: 5, 15, 16, 18,...,47

表 12 の行列に当てはめ、素数基底 P の各素数のベキ指数を計算し、正は左辺に、負は右辺にすると下記の関係式が得られる。

$$(2^6 \cdot 5^2 \cdot 7^3 \cdot 13^3 \cdot 29 \cdot 31 \cdot 37 \cdot 53 \cdot 79 \cdot 83 \cdot 89 \cdot 113 \cdot 149 \cdot 1597 \cdot 2311)^2 \equiv (3^2 \cdot 17 \cdot 67)^2 \pmod{18689147}$$

従って下記の関係となる。

$$10251^2 \equiv 10251^2 \pmod{18689147}$$

これは、自明解であり因数分解できない。

(2) 従属行 2： 4, 5, 11, 16,...,45

同様に下記の関係が得られる。

$$6856721^2 \equiv 6856721^2 \pmod{18689147}$$

これは、自明解であり因数分解できない。

(3) 従属行 3： 2, 4, 5, 7,...,49

同様に下記の関係が得られる。

$$2754620^2 \equiv 2011435^2 \pmod{18689147}$$

従って、$GCD(2754620 - 2011435, 18689147) = 7823$ から下記のように因数分解される。

$$18689147 = 7823 \cdot 2389$$

(4) 従属行 4： 2, 6, 8, 9

同様に下記の関係が得られる。

$$1981758^2 \equiv 1981758^2 \pmod{18689147}$$

これは、自明解であり因数分解できない。

(5) 従属行 5： 4, 5, 11, 14,...,51

同様に下記の関係が得られる。

$$8037499^2 \equiv 473925^2 \pmod{18689147}$$

従って、$GCD(8037499 - 473925, 18689147) = 2389$ から下記のように因数分解される。

$$18689147 = 2389 \cdot 7823$$

(6) 従属行 6： 1, 44

同様に下記の関係が得られる。

$$1063^2 \equiv 1063^2 \pmod{18689147}$$

これは、自明解であり因数分解できない。

(7) 従属行 7： 3, 5, 7, 9,…,53

同様に下記の関係が得られる。

$$5439295^2 \equiv 2868731^2 \pmod{18689147}$$

従って、$GCD(5439295-2868731,18689147)=2389$ から下記のように因数分解される。

$$18689147 = 2389 \cdot 7823$$

(8) 従属行 8： 1, 3, 5, 13,…,54

同様に下記の関係が得られる。

$$4764786^2 \equiv 4764786^2 \pmod{18689147}$$

これは、自明解であり因数分解できない。

(9) 従属行 9： 1, 5, 9, 12,…,55

同様に下記の関係が得られる。

$$3773254^2 \equiv 3773254^2 \pmod{18689147}$$

これは、自明解であり因数分解できない。

(10) 従属行 10： 2, 4,8,9,…,56

同様に下記の関係が得られる。

$$166956^2 \equiv 396300^2 \pmod{18689147}$$

従って、$GCD(396300-166956,18689147)=2389$ から下記のように因数分解される。

$$18689147 = 2389 \cdot 7823$$

(11) 従属行 11： 3, 7, 10, 11,…,57

同様に下記の関係が得られる。

$$1430080^2 \equiv 1430080^2 \pmod{18689147}$$

これは、自明解であり因数分解できない。

(12) 従属行 12： 1, 2, 3, 4,…,58

同様に下記の関係が得られる。

$$166956^2 \equiv 396300^2 \pmod{18689147}$$

従って、$GCD(396300-166956,18689147)=2389$ から下記のように因数分解される。

$$18689147 = 2389 \cdot 7823$$

(13) 従属行 13： 4, 5, 7, 10,…,59

同様に下記の関係が得られる。

$$6631743^2 \equiv 6631743^2 \pmod{18689147}$$

これは、自明解であり因数分解できない。

(14) 従属行 14： 1, 3, 4, 11,…,60

同様に下記の関係が得られる。

$$8115972^2 \equiv 6222806^2 \pmod{18689147}$$

従って、$GCD(8115972-6222806,18689147)=7823$ から下記のように因数分解される。

$$18689147 = 7823 \cdot 2389$$

(15) 従属行 15： 1, 3, 4, 8,…,61

同様に下記の関係が得られる。

$$3810128^2 \equiv 327^2 \pmod{18689147}$$

従って、$GCD(3810128-327,18689147)=7823$ から下記のように因数分解される。

$$18689147 = 7823 \cdot 2389$$

(16) 従属行 16： 2, 7, 8, 9, 10,…,62

同様に下記の関係が得られる。

$$1393853^2 \equiv 6040715^2 \pmod{18689147}$$

従って、$GCD(6040715-1393853,18689147)=7823$ から下記のように因数分解される。

$$18689147 = 7823 \cdot 2389$$