2 次の DBPS2 に因数分解例 1

2006/10/28　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

$N=55751$ 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. ふるい

詳細は「2 次の DBPS2 によるふるい例 1」を参照。

3.1 素数基底(P)

-1 及び 29 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 }

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 β_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。

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

(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	$2\cdot13^2$
項番	$x + b_2$	値(M_2+b_2)	M_2+b_2 の P での分解
1	x − 2	165	$3\cdot5\cdot11$
2	x − 1	166	$2\cdot83$
3	x	167	167
4	x + 1	168	$2^3\cdot3\cdot7$
5	x + 2	169	13^2

(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	$2^3\cdot29$
2	x − 3	233	233
3	x − 2	234	$2\cdot3^2\cdot13$
4	x	236	$2^2\cdot59$
5	x + 2	238	$2\cdot7\cdot17$
6	x + 3	239	239
7	x + 4	240	$2^4\cdot3\cdot5$

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、$|s_k| \le 2$ となるものだけ採用する。

(1) $f_1(x)$ に対するふるい結果

表 4 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 4. $f_1(x)$ 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· 19
6	3	-1	-2	1	-3	1	133	7· 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· 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	-----

(2) $f_2(x)$ に対するふるいデータの選定

表 5 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 5. $f_2(x)$ 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

(3) $f_3(x)$ に対するふるいデータの選定

表 6 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 6. $f_3(x)$ 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	-----

3.4 ふるい結果による行列

表 4,5,6 から 27×23 次元の行列ができるが、3 つの素数は 1 回しか使用されないため、これを削除すると 24×20 次元の行列が得られる。このとき、素数基底 P は 3 個除き下記の 20 個となり、その順に行列の列に対応する。

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

表 7 にふるい結果得られた行列を示す。

表 7. ふるい結果得られた行列

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

4. 行列の従属行の計算

(1) 0-1 行列の作成

表 7 の行列の各要素に対して (mod 2) を実施した結果を表 8 に示す。

表 8. 0-1 行列

A =

0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
0	0	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0
1	1	1	0	1	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0
1	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	1	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
0	1	1	1	0	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0
0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
1	0	1	1	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0
1	1	1	0	0	0	1	0	0	1	0	1	0	0	0	0	1	0	0	0
0	1	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
0	1	1	0	1	0	0	0	0	0	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
1	0	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0
0	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	1	1	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	1	1
0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
1	1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1
1	1	0	0	0	0	1	1	0	0	0	1	0	1	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 9 に示す。

表 9. (A+I)のガウス消去結果(A が完全消去された I の部分)

	列番号																							
	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	2	2	2	2	2
	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4
19	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	1	0	1	1	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	1	0	1	0	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	1	0	0	0
22	0	0	0	1	0	0	0	0	0	0	1	0	1	1	0	1	1	0	0	1	0	1	0	0
23	0	0	1	0	0	0	1	1	0	0	0	0	0	1	0	1	1	0	1	1	0	0	1	0
24	0	1	1	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	1

(3) 従属行

表 9 から 6 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 6 組の従属関係が得られる。

(a) 従属行 1： 2, 3, 4, 5, 6

(b) 従属行 2： 1, 3, 4, 5, 8, 9, 10

(c) 従属行 3： 2, 4, 11, 13, 14, 16, 18, 19, 20, 21

(d) 従属行 4： 4, 11, 13, 14, 16, 17, 20, 22

(e) 従属行 5： 3, 7, 8, 14, 16, 17, 19, 20, 23

(f) 従属行 6： 2, 3, 4, 9, 11, 17, 24

5. 因数分解

(1) 従属行 1: 2, 3, 4, 5, 6

表 7 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。

$$(3^4 \cdot 5 \cdot 11 \cdot 37 \cdot 137^2)^2 \equiv (2^4 \cdot 7 \cdot 19)^2 \pmod{55751}$$

従って下記の関係となる。

$$2128^2 \equiv 2128^2 \pmod{55751}$$

これは、自明解であり因数分解できない。

(2) 従属行 2： 1, 3, 4, 5, 8, 9, 10

同様に下記の関係が得られる。

$$17955^2 \equiv 17955^2 \pmod{55751}$$

これは、自明解であり因数分解できない。

(3) 従属行 3： 2, 4, 11, 13, 14, 16, 18, 19, 20, 21

同様に下記の関係が得られる。

$$12247^2 \equiv 361^2 \pmod{55751}$$

従って、$GCD(12247-361,55751)=283$ から下記のように因数分解される。

$$55751 = 283 \cdot 197$$

(4) 従属行 4： 4, 11, 13, 14, 16, 17, 20, 22

同様に下記の関係が得られる。

$$19010^2 \equiv 1083^2 \pmod{55751}$$

従って、$GCD(19010-1083,55751)=197$ から下記のように因数分解される。

$$55751 = 197 \cdot 283$$

(g) 従属行 5： 3, 7, 8, 14, 16, 17, 19, 20, 23

同様に下記の関係が得られる。

$$7465^2 \equiv 176^2 \pmod{55751}$$

従って、$GCD(7465-176,55751)=197$ から下記のように因数分解される。

$$55751 = 197 \cdot 283$$

(6) 従属行 6： 2, 3, 4, 9, 11, 17, 24

同様に下記の関係が得られる。

$$19^2 \equiv 19^2 \pmod{55751}$$

これは、自明解であり因数分解できない。