2 次の DBPS(2 重基底多項式篩法)による篩例

2006/5/25 後 保範
2006/5/30 改 定

1. 概要

合成数 N に対して 2 次関数 $f(x)$ を使用して篩を行い、因数分解する。

$f(x)=Ax^2+Bx+C,\ f(M)\equiv 0 \pmod N$ に対して下記の様に関数 $g(x)$ を定義する。

$$g(x)=(cAx+a)(dx+b)-cdf(x)=sx+t$$
$$s=ad+c(bA-dB),\ t=ab-cdC$$

すると、関数 $f(x)$ と数値 N に対する剰余が下記で与えられる。

$$g(x)=(cAx+a)(dx+b)\equiv sx+t \pmod{f(x)} \quad \text{--- (1)}$$
$$(cAM+a)(dM+b)\equiv sM+t \pmod N \quad \text{--- (2)}$$

(2)式に素数と一次式の 2 つの基底を使用して篩をおこなう。

即ち、素数基底と一次式基底を使用して、$cAM+a, dM+b$ 及び $sM+t$ を篩により分解する。素数基底は-1 と小さい素数より順に選ぶ。一次式基底は素数基底で分解できない $\alpha M+\beta$ で、α,β の値が小さく出現頻度が多いもの順に選ぶ。

本方式を MBPS(Multiple Base Polynomial Sieve、多重基底多項式篩法)の一種の DBPS(Double Base Polynomial Sieve、2 重基底多項式篩法)と名付ける。

DBPS は MPQS と同様に多数の関数 $f(x)$ を使用できる。

2. 計算対象

$N=55751$ を MPBS で篩を行い因数分解する。

篩には下記の多項式 $f(x)$ を使用する。説明を簡単にするため 1 個の関数だけ使用する。

$$f(x)=2x^2-27,\ f(M)=N,\ M=167$$

素数基底は-1 と 2,3,5,7,11,13,17,19,23 の 9 個の素数を使用する。

一次式基底は M-3,M,2M+1,2M+3 及び 2M+5 の 5 個を使用する。

3. 篩の準備

$c=1, d=1$ かつ、a,b,s の絶対値が 9 以下のもので篩を行う。そのために必要な、$M+b$ 及び $2M+a$ が素数基底で分解されるものを選ぶ。表 1 に素数基底で分解できるものを示す。

表 1. 素数基底で分解できる M の一次式

M+b の分解			2M+a の分解		
一次式	値	基底での分解	一次式	値	基底での分解
M - 7	160	$2^5\cdot 5$	2M - 9	325	$5^2\cdot 13$
M - 6	161	$7\cdot 23$	- - -	- - -	- - -
M - 5	162	$3\cdot 2^4$	- - -	- - -	- - -

M - 2	165	$3\cdot5\cdot11$	2M-4=2(M-2)	330	$2\cdot3\cdot5\cdot11$
M+1	168	$2^3\cdot5\cdot17$	2M+2=2(M+1)	336	$2^4\cdot5\cdot17$
M+2	169	13^2	2M+4=2(M+2)	338	$2\cdot13^2$
M+3	170	$2\cdot5\cdot17$	2M+6=2(M+3)	340	$2\cdot5\cdot17$
M+4	171	$3^2\cdot19$	2M+8=2(M+4)	342	$2\cdot3^2\cdot19$
M+8	175	$5\cdot7^2$	- - -	- - -	- - -
M+9	176	$2^4\cdot11$	2M+9	343	7^3

4. 篩の実行

$c=1, d=1$かつ、a,b,sの絶対値が 9 以下のもので篩を行う。そのため、(2)式の左辺は一次式基底及び、表 1 に現れる一式だけで構成されるものだけで篩を行う。右辺は素数基底と一次式基底で分解テストを行う。篩では$(2M+a)(M+b)$が既に現われた式の倍数は最初から対象にしない。例えば$(2M+0)(2M+0)$は$(2M+0)(M+0)$の倍数のため、篩の対象から除く。表 2 に篩の実行過程を示す。表 2 の斜体の数字及び一次式は素数基底で分解できるものを示す。

表 2. 篩の実行過程(c=d=1)

番号	g(x)の係数				sM+t の値	sM+t の基底での分解結果	篩結果 No.
	a	b	s	t			
1	0	*4*	8	27	1363		
2	0	*3*	6	27	1029	$3(2M+9)=3\cdot7^3$	1
3	0	*2*	4	27	695		
4	0	*1*	2	27	361	19^2	2
5	0	0	0	27	27	3^3	3
6	0	*-2*	-4	27	-641		
7	0	-3	-6	27	-975	$-3(2M-9)=-3\cdot5^2\cdot13$	4
8	1	*4*	9	31	1534		
9	1	*3*	7	30	1199		
10	1	*2*	5	29	864	$2^5\cdot3^3$	5
11	1	*1*	3	28	529	23^2	6
12	1	0	1	27	194		
13	1	*-2*	-3	25	-476	$-2^2\cdot7\cdot17$	7
14	1	-3	-5	24	-811		
15	1	*-5*	-9	22	-1481		
16	*2*	*3*	8	33	1369		
17	*2*	*2*	6	31	1033		
18	*2*	*1*	4	29	697		
19	*2*	*-2*	-2	23	-311		
20	*2*	-3	-4	21	-647		
21	*2*	*-5*	-8	17	-1319		
22	3	*3*	9	36	1539	$9(M+4)=3^4\cdot19$	8
23	3	*2*	7	33	1202		

24	3	*1*	5	30	865		
25	3	0	3	27	528	$3(M+9)=2^4 \cdot 3 \cdot 11$	9
26	3	*-2*	-1	21	-146		
27	3	-3	-3	18	-483	$-3(M+6)=-3 \cdot 7 \cdot 23$	10
28	3	*-5*	-7	12	-1157		
29	3	*-6*	-9	9	1494		
31	*4*	*2*	8	35	1371		
32	*4*	*-2*	0	19	19	*19*	11
33	*4*	-3	-2	15	-319		
34	*4*	*-5*	-6	7	-995		
35	*4*	*-6*	-8	3	-1333		
36	*-4*	*4*	4	11	697		
37	*-4*	*3*	2	15	349		
38	5	*2*	9	37	1540	$2^2 \cdot 5 \cdot 7 \cdot 11$	12
39	5	*1*	7	32	1201		
40	5	0	5	27	862		
41	5	*-2*	1	17	184	$2^3 \cdot 23$	13
42	5	-3	-1	12	-155		
43	5	*-5*	-5	2	-833	$-7^2 \cdot 17$	14
44	5	*-6*	-7	-3	-1172		
45	5	*-7*	-9	-8	-1511		
46	*6*	*-3*	0	9	9	3^2	15
47	*6*	*-5*	-4	-3	-671		
48	*6*	*-6*	-6	-9	-1011	-3(2M+3)	16
49	*6*	*-7*	-8	-15	-1351		
50	*8*	*-5*	-2	-13	-347		
51	*8*	*-6*	-4	-21	-689		
52	*8*	*-7*	-6	-29	-1031		
53	*9*	0	9	27	1530	$9(M+3)=2 \cdot 3^2 \cdot 5 \cdot 17$	17
54	*9*	*-2*	5	9	844		
55	*9*	-3	3	0	501	3M	18
56	*9*	*-5*	-1	-18	-185		
57	*9*	*-6*	-3	-27	-528	$-3(M+9)=-2^4 \cdot 3 \cdot 11$	19
58	*9*	*-7*	-5	-36	-871		
59	*-9*	*9*	9	-54	1449	$9(M-6)=3 \cdot 27 \cdot 23$	20
60	*-9*	*8*	7	-45	1124		
61	*-9*	*4*	-1	-9	-176	$-(M+9)=-2^4 \cdot 11$	21
62	*-9*	3	-3	0	-501	-3M	22
63	*-9*	*2*	-5	-9	-826		
64	*-9*	*1*	7	18	-1151		
65	*-9*	*0*	-9	27	-1476		

本 DBPS の最大の特長は、篩に一次式基底を導入し、一次式基底による分解は GNFS(一般数体篩法)の素イデアルでの分解と異なり、自然に(2)式で求まることである。また、左辺と

右辺に現われる一次式は共に一次式基底で処理できる。更に、左辺側の一次式は同一なものが多量に出現する。この性質により、多数桁数の因数分解で GNFS より高速化できると思われる。また、多数桁数の因数分解での篩において、GNFS の素数基底、素イデアル基底及び平方剰余を合わせた数より、DBPS の素数基底と一次基底を合わせた数が大幅に少なくできると思われる。このため、その後の行列計算も GNFS より高速化できると考えられる。

5. 篩の結果

表 2 による篩の実行過程から、$sM+t$ が素数基底及び一次式基底で分解されたものを選び出す。表 2 の篩結果 No.に番号を入れたものが DBPS による篩結果である。素数と一次式の両基底の合計は 15 個であり、選定された篩結果は 22 個あり、これは N が分解されるための条件を満たす。

表 3 に篩結果の行列を示す。表 2 の No は表 2 の篩結果 No に対応する。表 3 中の一次式基底の B1,B2,B3,B4 及び B5 はそれぞれ M-3,M,2M+1,2M+3 及び 2M+5 に対応する。表 3 の正のベキは左辺での指数を、負のベキは右辺での指数を示す。従って、表 1 の No.1～No.4 は(mod N)の基で下記の等式を示す。No.5 以下も同様である。

No.1 : $2M(M+3) \equiv 3(2M+9) \rightarrow 2^2 \cdot 5 \cdot 17 \cdot M \equiv 3 \cdot 7^3$

No.2 : $2M(M+1) \equiv 2M+27 \rightarrow 2^4 \cdot 3 \cdot 7 \cdot M \equiv 19^2$

No.3 : $2M^2 \equiv 27 \rightarrow 2 \cdot M^2 \equiv 3^3$

No.4 : $2M(M-3) \equiv -3(2M-9) \rightarrow 2 \cdot (M-3) \cdot M \equiv -1 \cdot 3 \cdot 5^2 \cdot 13$

表 3. 2 次の DBPS による篩結果の行列 (c,d=1)

No	g(x)の係数		mod N での等式														
			素数基底										一次式基底				
	a	b	-1	2	3	5	7	11	13	17	19	23	B1	B2	B3	B4	B5
1	0	3	0	2	-1	1	-3	0	0	1	0	0	0	1	0	0	0
2	0	1	0	4	1	0	1	0	0	0	-2	0	0	1	0	0	0
3	0	0	0	1	-3	0	0	0	0	0	0	0	0	2	0	0	0
4	0	-3	1	1	-1	-2	0	0	-1	0	0	0	1	1	0	0	0
5	1	2	0	-5	-3	0	0	0	2	0	0	0	0	0	1	0	0
6	1	1	0	3	1	0	1	0	0	0	0	-2	0	0	1	0	0
7	1	-2	1	-2	1	1	-1	1	0	-1	0	0	0	0	1	0	0
8	3	3	0	1	-4	1	0	0	0	1	-1	0	0	0	0	1	0
9	3	0	0	-4	-1	0	0	-1	0	0	0	0	0	1	0	1	0
10	3	-3	1	0	-1	0	-1	0	0	0	0	-1	1	0	0	1	0
11	4	-2	0	1	1	1	0	1	2	0	-1	0	0	0	0	0	0
12	5	2	0	-2	0	-1	-1	-1	2	0	0	0	0	0	0	0	1
13	5	-2	0	-3	1	1	0	1	0	0	0	-1	0	0	0	0	1
14	5	-5	1	1	4	0	-2	0	0	-1	0	0	0	0	0	0	1
15	6	-3	0	2	-2	1	0	0	0	1	0	0	1	0	0	0	0
16	6	-6	1	2	-1	1	1	0	0	1	0	1	0	0	0	-1	0

17	9	0	0	-1	-2	-1	3	0	0	-1	0	0	0	1	0	0	0
18	9	-3	0	0	-1	0	3	0	0	0	0	0	1	-1	0	0	0
19	9	-6	1	-4	-1	0	4	-1	0	0	0	1	0	0	0	0	0
20	-9	9	0	4	-2	2	-1	1	1	0	0	-1	0	0	0	0	0
21	-9	4	1	-4	2	2	0	-1	1	0	1	0	0	0	0	0	0
22	-9	3	1	1	-1	3	0	0	1	1	0	0	0	-1	0	0	0

6. 篩を使用した因数分解

表 1 を使用して、N を因数分解する方法は「2 次の DBPS による因数分解例」を参照。

最終的に N は $N = 55751 = 197 \cdot 283$ と分解される。