2 次の TBPS2 によるふるい例

2006/08/16　後 保範

1. 概要

TBPS(3 重基底多項式篩法)を改良した TBPS2(Triple Base Polynomial Sieve 2nd)を使用して因数分解する例を示す。

$f(x)=Ax^2+Bx+C,\ f(M)\equiv 0 \pmod N$ となる、2 次多項式 $f(x)$ と整数 M を求める。このとき、TBPS2 では $A\theta+a$ 及び $\theta+b$ が共に素イデアル基底で分解されるなら、$s\theta+t$ もまた素イデアル基底で分解される性質を利用するのが特長である。

2. 分解対象と使用多項式

N=55751 を素因数分解する。

下記の多項式を使用してふるいを行う。

$f(x)=3x^2+2x-9,\quad M=136,\quad f(M)=N$

3. 基本基底

(1) 素数基底

-1 及び 19 以下の素数で基本素数基底 P1 を構成する。

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

(2) 素イデアル基底

P1 の素数 p に対応する素イデアルを $f(s)\equiv 0 \pmod p$ が成立する、基本素イデアル基底 Q1 を求める。素イデアル基底は $(p:s)$ のペアーで表示する。

Q1 = {(2:1), (3:1), (7:2), (19:5,7)}

4. 追加基底と $Ax+a, x+b$ の選定

(1) 選定基準

$|a|\le 3, |b|\le 2$ の範囲で、$3M+a, M+b$ の全てが分解されるように追加素数基底を選ぶ。

更に、イデアル $3\theta+a, \theta+b$ も全て分解されるように素イデアル基底を選ぶ。

(2) 選定

選定する素数の上界を 500 とする。今回の場合はこの条件は全てクリアする。

表 1 に $x+b$ と $3x+a$ の基本素数基底 P1 と基本素イデアル基底 Q1 での分解結果と、P1 及び Q1 で分解できない値(因子)を示す。

表 1.　$Ax+a, x+b$ の分解結果

素数分解				素イデアル分解				
整数式	値 (V)	P1 での分解 (累計値:T)	因子 (V/T)	共通値	イデアル式	ノルム (U)	Q1 での分解 (累計値:R)	因子 (U/R)
M-2	134	2	67	1	$\theta-2$	7	7	1
M-1	135	$3^3\cdot 5=135$	1	1	$\theta-1$	4	$2^2=4$	1
M	136	$2^3\cdot 17=136$	1	1	θ	9	$3^2=9$	1
M+1	137	137	137	1	$\theta+1$	8	$2^3=8$	1
M+2	138	$2\cdot 3=6$	23	1	$\theta+2$	1	1	1
3M-3	405	$3^4\cdot 5=405$	1	3	$\theta-1$	4	$2^2=4$	1
3M-2	406	$2\cdot 7=14$	29	1	$3\theta-2$	57	$3\cdot 19=57$	1
3M-1	407	11	37	1	$3\theta-1$	72	$2^3\cdot 3^2=72$	1
3M	408	$2^3\cdot 3\cdot 17=408$	1	3	θ	9	$3^2=9$	1
3M+1	409	1	409	1	$3\theta+1$	84	$2^2\cdot 3\cdot 7=84$	1
3M+2	410	$2\cdot 5=10$	41	1	$3\theta+2$	81	$3^4=81$	1
3M+3	411	3	137	3	$\theta+1$	8	$2^3=8$	1

注）イデアル $c\theta+d$ に対するノルムは $N(c\theta+d)=|Ad^2-Bcd+Cc^2|$ で求める。

(3) 追加基底のまとめ

追加素数基底 P2 は表 1 の素数分解の因子から下記のようになる。

P2 = {23, 29, 37, 41, 67, 137, 409}

従って、P1 と P2 を合わせた素数基底 P は下記のようになり、-1 から 409 を順に P_1 から P_{16} で表す。

P = {-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 67, 137, 409}

今回は、追加素イデアル基底 Q2 は存在しない。従って、素イデアル基底 Q は

Q = {Q_1, Q_2, Q_3, Q_4}とする。

ここで、Q1=(2:1), Q2=(3:1), Q3=(7:2), Q4=(19:5,7)である。

5. GNFS による基本区間のふるい

ここでは、ふるい結果を述べる。ふるいの詳細は「GNFS による篩例」を参照。

イデアル $c\theta+d$ で、$c=1,2,3$ かつ $|d|\le 15$ の範囲でのふるい結果を表 2 に示す。

GNFS のふるい結果として採用するのは、整数 $cM+d$ が素数基底 P で分解され、イデアル $c\theta+d$ が素イデアル基底 Q で共に分解される場合である。

表 2. 基本区間の GNFS ふるい結果

NO.	イデアル	素数分解		素イデアル分解	
	$c\theta+d$	$cM+d$	P での分解	$N(c\theta+d)$	Q での分解
1	$\theta-3$	133	$7\cdot 19$	24	$2^3\cdot 3$
2	$\theta-2$	134	$2\cdot 67$	7	7
3	$\theta-1$	135	$3^3\cdot 5$	4	2^2
4	θ	136	$2^3\cdot 17$	9	3^2
5	$\theta+1$	137	137	8	2^3
6	$\theta+2$	138	$2\cdot 3\cdot 23$	1	1
7	$\theta+9$	145	$5\cdot 29$	216	$2^3\cdot 3^3$
8	$\theta+12$	148	$3^2\cdot 37$	399	$3\cdot 7\cdot 19$
9	$2\theta+3$	275	$5^2\cdot 11$	21	$3\cdot 7$
10	$3\theta-2$	406	$2\cdot 7\cdot 29$	57	$3\cdot 19$
11	$3\theta-1$	407	$11\cdot 37$	72	$2^3\cdot 3^2$
12	$3\theta+1$	409	409	84	$2^2\cdot 3\cdot 7$
13	$3\theta+2$	410	$2\cdot 5\cdot 41$	81	3^4
14	$3\theta+8$	416	$2^5\cdot 13$	63	$3^2\cdot 7$

6. DBPS による主ふるい

表 1 で選定した、$Ax+a$ と $x+b$ より下記の式で、s,t を計算する。

$$sx+t=(Ax+a)\cdot(x+b)-f=(Ab+a-B)x+ab-C$$

$$s=Ab+a-B,\quad t=ab-C$$

s,t の最大公約数 G 及び s,t を G で除した S,T を下記で求める。

$$G=sign(s)\cdot GCD(|s|,|t|)$$

$$S=s/G,\quad T=t/G$$

そこで、$1\le S\le 3$ かつ $|T|\le 15$、又は $s=0$ で t が素数基底で分解できるものを選ぶ。

表 3 に DBPS による主ふるいを示す。採否が○のものをふるい結果として採用する。

表 3. DBPS による主ふるい

NO.	入力		出力			採否
	$3x+a$	$x+b$	$sx+t$	G	$Sx+T$	
1	$3(x-1)$	$x-2$	$-11x+15$	−1	$11x-15$	×
2	$3(x-1)$	$x-1$	$-8x+12$	−4	$2x-3$	○
3	$3(x-1)$	x	$-5x+9$	−1	$5x-9$	×
4	$3(x-1)$	$x+1$	$-2x+6$	−2	$x-3$	○

5	$3(x-1)$	$x+2$	$x+3$	1	$x+3$	○
6	$3x-2$	$x-2$	$-10x+13$	−1	$10x-13$	×
7	$3x-2$	$x-1$	$-7x+11$	−1	$7x-11$	×
8	$3x-2$	x	$-4x+9$	−1	$4x-9$	×
9	$3x-2$	$x+1$	$-x+7$	−1	$x-7$	○
10	$3x-2$	$x+2$	$2x+5$	1	$2x+5$	○
11	$3x-1$	$x-2$	$-9x+11$	−1	$9x-11$	×
12	$3x-1$	$x-1$	$-6x+10$	−2	$3x-5$	○
13	$3x-1$	x	$-3x+9$	−3	$x-3$	○
14	$3x-1$	$x+1$	8	1	8	○
15	$3x-1$	$x+2$	$3x+7$	1	$3x+7$	○
16	$3x$	$x-2$	$-8x+9$	−1	$8x-9$	×
17	$3x$	$x-1$	$-5x+9$	−1	$5x-9$	×
18	$3x$	x	$-2x+9$	−1	$2x-9$	○
19	$3x$	$x+1$	$x+9$	1	$x+9$	○
20	$3x$	$x+2$	$4x+9$	1	$4x+9$	×
21	$3x+1$	$x-2$	$-7x+7$	−7	$x-1$	○
22	$3x+1$	$x-1$	$-4x+8$	−2	$2x-4$	○
23	$3x+1$	x	$-x+9$	−1	$x-9$	○
24	$3x+1$	$x+1$	$2x+10$	2	$x+5$	○
25	$3x+1$	$x+2$	$5x+11$	1	$5x+11$	×
26	$3x+2$	$x-2$	$-6x+5$	−1	$6x-5$	×
27	$3x+2$	$x-1$	$-3x+7$	−1	$3x-7$	○
28	$3x+2$	x	9	1	9	○
29	$3x+2$	$x+1$	$3x+11$	1	$3x+11$	○
30	$3x+2$	$x+2$	$6x+13$	1	$6x+13$	×
31	$3(x+1)$	$x-2$	$-5x+3$	−1	$5x-3$	×
32	$3(x+1)$	$x-1$	$-2x+6$	−2	$x-3$	○
33	$3(x+1)$	x	$x+9$	1	$x+9$	○
34	$3(x+1)$	$x+1$	$4x+12$	4	$x+3$	○
35	$3(x+1)$	$x+2$	$7x+15$	1	$7x+15$	×

7. 主ふるいのソートと重複除去

表 3 を出力の $Sx+T, G$ で上昇順にソートする。

その結果、$G\cdot(Sx+T)$ が $-2(x-3)$ 及び $x+9$ が 2 度現れる。そのため、NO. 32 及び

NO.33 を重複除去する。

8. 行列の作成

表 2 及び表 3 のふるい結果(ソートし重複除去)より表 4 の行列が得られる。
各要素の素数基底(P)及び素イデアル基底(Q)での分解は表 1 を使用して行う。
このとき、表 3 の G の値は素数基底の素数分解の位置に逆数(G^{-1})の形で入れる。

表 4. TBPS によるふるい結果の行列

NO.	素数基底		素イデアル基底	
	一次式値	素数分解	イデアル	素イデアル分解
1	133	$7\cdot 19$	$\theta-3$	$2^3\cdot 3$
2	134	$2\cdot 67$	$\theta-2$	7
3	135	$3^3\cdot 5$	$\theta-1$	2^2
4	136	$2^3\cdot 17$	θ	3^2
5	137	137	$\theta+1$	2^3
6	138	$2\cdot 3\cdot 23$	$\theta+2$	1
7	145	$5\cdot 29$	$\theta+9$	$2^3\cdot 3^3$
8	148	$3^2\cdot 37$	$\theta+12$	$3\cdot 7\cdot 19$
9	275	$5^2\cdot 11$	$2\theta+3$	$3\cdot 7$
10	406	$2\cdot 7\cdot 29$	$3\theta-2$	$3\cdot 19$
11	407	$11\cdot 37$	$3\theta-1$	$2^3\cdot 3^2$
12	409	409	$3\theta+1$	$2^2\cdot 3\cdot 7$
13	410	$2\cdot 5\cdot 41$	$3\theta+2$	3^4
14	416	$2^5\cdot 13$	$3\theta+8$	$3^2\cdot 7$
15	$137\cdot 407$	$2^{-3}\cdot 11\cdot 37\cdot 137$	1	1
16	$136\cdot 410$	$2^4\cdot 3^{-2}\cdot 5\cdot 17\cdot 41$	1	1
17	$136\cdot 409$	$-1\cdot 2^3\cdot 3\cdot 17\cdot 409$	$\theta-9$	$2^2\cdot 3^2\cdot 7$
18	$137\cdot 406$	$-1\cdot 2\cdot 7\cdot 29\cdot 137$	$\theta-7$	$2^3\cdot 19$
19	$136\cdot 407$	$-1\cdot 2^3\cdot 3^{-1}\cdot 11\cdot 17\cdot 37$	$\theta-3$	$2^3\cdot 3$
20	$3\cdot 135\cdot 137$	$-1\cdot 2^{-1}\cdot 3^4\cdot 5\cdot 137$	$\theta-3$	$2^3\cdot 3$
21	$135\cdot 409$	$-1\cdot 2^{-2}\cdot 3^3\cdot 5\cdot 409$	$\theta-2$	7
22	$134\cdot 409$	$-1\cdot 2\cdot 7^{-1}\cdot 67\cdot 409$	$\theta-1$	2^2
23	$3\cdot 135\cdot 138$	$2\cdot 3^5\cdot 5\cdot 23$	$\theta+3$	$2^2\cdot 3$
24	$3\cdot 137^2$	$2^{-2}\cdot 3\cdot 137^2$	$\theta+3$	$2^2\cdot 3$
25	$137\cdot 409$	$2^{-1}\cdot 137\cdot 409$	$\theta+5$	$2^3\cdot 7$

26	$3\cdot 136\cdot 137$	$2^3\cdot 3\cdot 17\cdot 137$	$\theta+9$	$2^3\cdot 3^3$
27	$3\cdot 136^2$	$-1\cdot 2^6\cdot 3\cdot 17^2$	$2\theta-9$	3^5
28	$3\cdot 135^2$	$-1\cdot 2^{-2}\cdot 3^7\cdot 5^2$	$2\theta-3$	3
29	$138\cdot 406$	$2^2\cdot 3\cdot 7\cdot 23\cdot 29$	$2\theta+5$	19
30	$135\cdot 410$	$-1\cdot 2\cdot 3^3\cdot 5^2\cdot 41$	$3\theta-7$	$2^2\cdot 3^3$
31	$135\cdot 407$	$-1\cdot 2^{-1}\cdot 3^3\cdot 5\cdot 11\cdot 37$	$3\theta-5$	$2^3\cdot 3$
32	$138\cdot 407$	$2\cdot 3\cdot 11\cdot 23\cdot 37$	$3\theta+7$	$2^3\cdot 3$
33	$137\cdot 410$	$2\cdot 5\cdot 41\cdot 137$	$3\theta+11$	$2^3\cdot 3^3$

更に、23 以上の素数 p に対応する平方剰余 R を $f(s)\equiv 0 \pmod{p}$ が成立するように、下記のように 6 個定める。各 R は($p:s$)を表す。

R_1=(29:−14)， R_2=(31:−7)， R_3=(37:6)， R_4=(47:4)， R_5=(53:−21)， R_6=(59:−27)

表 4 のイデアル $c\theta+d$ に対して、各 R($p:s$)で平方剰余になるか非平方剰余になるか調べ、平方剰余なら 0 を非平方剰余なら 1 とする。平方剰余のテストは $a-bs$ が p の平方剰余かどうか、即ち $(a-bs)^{p-1} \pmod{p}$ を計算し、その結果が 1 なら 0 を−1 なら 1 とする。 $a-bs$ が p の倍数なら平方剰余で 0 とする。表 4 の各項に対して 16 個の素数基底 P(P_1～P_{16})、4 個の素イデアル基底 Q(Q_1～Q_4)及び 6 個の平方剰余 R(R_1～R_6)の合計 26 個を列とした 33×26 の行列を作成する。ここで、P_1～P_{16} 及び Q_1～Q_4 に対応するものは、そのベキ数の $\pmod 2$ の値を入れる。表 5 に上記で作成した 0-1 行列を示す。

表 5. TBPS により作成した 0-1 行列

行番号	P_1, P_2, P_3, P_4, P_5 ～ P_{15}, P_{16}	Q_1～Q_4	R_1～R_6
1	0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0	1 1 0 0	1 0 0 1 1 1
2	0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0	0 0 1 0	1 0 1 1 1 0
3	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 0
4	0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0	0 0 0 0	1 0 1 1 1 0
5	0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0	1 0 0 0	1 0 1 1 1 0
6	0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0	0 0 0 0	0 0 0 1 1 0
7	0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0	1 1 0 0	0 0 0 1 1 0
8	0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0	0 1 1 1	1 0 1 0 1 1
9	0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0	0 1 1 0	1 1 0 0 1 0
10	0 1 0 0 1 0 0 0 0 0 1 0 0 0 0 0	0 1 0 1	1 0 1 1 1 0
11	0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0	1 0 0 0	1 0 1 0 0 0
12	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1	0 1 1 0	1 1 1 0 0 1
13	0 1 0 1 0 0 0 0 0 0 0 1 0 0 0 0	0 0 0 0	1 1 0 0 1 1
14	0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0	0 0 1 0	1 1 0 1 1 1
15	0 1 0 0 0 1 0 0 0 0 0 1 0 0 1 0	0 0 0 0	0 0 0 0 0 0
16	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
17	1 1 0 0 0 0 0 1 0 0 0 0 0 0 0 1	0 0 1 0	0 1 1 0 1 1

18	1 1 0 0 1 0 0 0 0 0 1 0 0 0 1 0	1 0 0 1	0 0 1 0 1 0
19	1 1 1 0 0 1 0 1 0 0 0 1 0 0 0 0	1 1 0 0	1 0 0 1 1 1
20	1 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0	1 1 0 0	1 0 0 1 1 1
21	1 0 1 1 0 0 0 0 0 0 0 0 0 0 0 1	0 0 1 0	1 0 1 1 1 0
22	1 1 0 0 1 0 0 0 0 0 0 0 0 1 0 1	0 0 0 0	0 1 0 0 1 0
23	0 1 1 1 0 0 0 0 0 1 0 0 0 0 0 0	0 1 0 0	1 0 0 1 0 1
24	0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 0 0	1 0 0 1 0 1
25	0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1	1 0 1 0	1 1 0 0 1 1
26	0 1 1 0 0 0 0 1 0 0 0 0 0 0 1 0	1 1 0 0	0 0 0 1 1 0
27	1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 0 0	1 0 0 1 1 0
28	1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 0 0	0 1 1 0 1 0
29	0 0 1 0 1 0 0 0 0 1 1 0 0 0 0 0	0 0 0 1	0 0 0 1 0 0
30	1 1 1 0 0 0 0 0 0 0 0 0 1 0 0 0	0 1 0 0	0 0 0 0 1 0
31	1 1 1 1 0 1 0 0 0 0 0 1 0 0 0 0	1 1 0 0	1 0 1 1 1 0
32	0 1 1 0 0 1 0 0 0 1 0 1 0 0 0 0	1 1 0 0	0 0 0 0 0 0
33	0 1 0 1 0 0 0 0 0 0 0 1 0 1 0	1 1 0 0	0 0 0 1 1 1

9. 因数分解

因数分解の途中経過は 2 次の TBPS2 による因数分解例を参照。

TBPS2 によるふるい結果から下記の因数分解が得られる。

(a) $1523^2 \equiv 1523^2 \pmod{55751}$ → 自明解のため因数分解不可

(b) $7323^2 \equiv 7323^2 \pmod{55751}$ → 自明解のため因数分解不可

(c) $8055^2 \equiv 15979^2 \pmod{55751}$ → 55751=197・283 と因数分解

(d) $8111^2 \equiv 19340^2 \pmod{55751}$ → 55751=197・283 と因数分解

(e) $10864^2 \equiv 5487^2 \pmod{55751}$ → 55751=197・283 と因数分解

(f) $4648^2 \equiv 23326^2 \pmod{55751}$ → 55751=197・283 と因数分解

(g) $398^2 \equiv 6111^2 \pmod{55751}$ → 55751=197・283 と因数分解

(h) $26834^2 \equiv 13635^2 \pmod{55751}$ → 55751=197・283 と因数分解

(i) $16392^2 \equiv 16392^2 \pmod{55751}$ → 自明解のため因数分解不可