2 次の TBPS(3 重基底多項式篩法)による因数分解例

2006/5/30 後 保範

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。

$$g(x)=(a_1Ax+b_1)(a_2x+b_2)-a_1a_2f(x)=sx+t$$

$$s=a_2b_1+a_1(b_2A-a_2B),\ \ t=b_1b_2-a_1a_2C$$

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。

$$g(x)=(a_1Ax+b_1)(a_2x+b_2)\equiv sx+t \pmod{f(x)} \quad \text{--- (1)}$$

$$(a_1AM+b_1)(a_2M+b_2)\equiv sM+t \pmod N \quad \text{--- (2)}$$

一方、$f(\theta)$ に対する GNFS(一般数体篩法)イデアルを $a\theta+b$ とすると、対応するノルム $h(a,b)$ は下記で与えられる。

$$h(a,b)=abs(Ab^2-Bab+Ca^2) \quad \text{--- (3)}$$

ここで、(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い、(3)式は素イデアル基底で篩をおこなう。イデアル $a\theta+b$ は $aM+b$ として、素数と一次式の 2 つの基底で篩をおこなう。即ち、素数基底と一次式基底を使用して、$a_1M+b_1, a_2M+b_2, sM+t$ 及び $aM+b$ を篩により分解する。更に、素イデアル基底で $h(a,b)$ を分解する。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 $\alpha M+\beta$ に対して、α,β が小さい整数で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)の中の一つの TBPS(Triple Base Polynomial Sieve、3 重基底多項式篩法)と名付ける。

TBPS の素イデアル基底の数は素数基底に比較し非常に少ないので、TBPS は GNFS とは異なり MPQS(複数多項式 2 次篩法)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 TBPS で因数分解する。

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,2M+1,2M+3 及び 2M+5 の 4 個を使用する。

素イデアル基底に対応する素数は 2,3,5,19 の 4 個を使用する。

3. 素数及び一次式による篩

$a_1=1,\ a_2=1$ かつ、b_1,b_2,s の絶対値が 9 以下のもので篩を行う。素数と一次式の基底の合

計は 14 で、篩の結果はそれより 4 個多く 18 個を選定した。そのため、この篩結果だけでも N は因数分解可能である。

表 1 に篩結果の行列を示す。表 1 中の一次式基底の B1,B2,B3 及び B4 はそれぞれ M,2M+1,2M+3 及び 2M+5 に対応する。表 1 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.3 は(mod N)の基で下記の等式を示す。No.4 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 : $2M^2 \equiv 27 \rightarrow 2 \cdot M^2 \equiv 3^3$

表 1. 2 次の TBPS による篩結果の行列 (a_1,a_2=1)

No.	g(x)の係数		mod N での等式													
			素数基底										一次式基底			
	b_1	b_2	-1	2	3	5	7	11	13	17	19	23	B1	B2	B3	B4
1	0	3	0	2	-1	1	-3	0	0	1	0	0	1	0	0	0
2	0	1	0	4	1	0	1	0	0	0	-2	0	1	0	0	0
3	0	0	0	1	-3	0	0	0	0	0	0	0	2	0	0	0
4	1	2	0	-5	-3	0	0	0	2	0	0	0	0	1	0	0
5	1	1	0	3	1	0	1	0	0	0	0	-2	0	1	0	0
6	1	-2	1	-2	1	1	-1	1	0	-1	0	0	0	1	0	0
7	3	3	0	1	-4	1	0	0	0	1	-1	0	0	0	1	0
8	3	0	0	-4	-1	0	0	-1	0	0	0	0	1	0	1	0
9	4	-2	0	1	1	1	0	1	2	0	-1	0	0	0	0	0
10	5	2	0	-2	0	-1	-1	-1	2	0	0	0	0	0	0	1
11	5	-2	0	-3	1	1	0	1	0	0	0	-1	0	0	0	1
12	5	-5	1	1	4	0	-2	0	0	-1	0	0	0	0	0	1
13	6	-6	1	2	-1	1	1	0	0	1	0	1	0	0	-1	0
14	9	0	0	-1	-2	-1	3	0	0	-1	0	0	1	0	0	0
15	9	-6	1	-4	-1	0	4	-1	0	0	0	1	0	0	0	0
16	-9	9	0	4	-2	2	-1	1	1	0	0	-1	0	0	0	0
17	-9	4	1	-4	2	2	0	-1	1	0	1	0	0	0	0	0
18	-9	3	1	1	-1	3	0	0	1	1	0	0	-1	0	0	0

4. 素イデアルによる篩

$f(x)$ のイデアル $a\theta + b$ に対して、$a = 1,2,3$ で b の絶対値が 11 以内で GNFS の篩をおこなう。このとき、$aM + b$ は素数基底及び一次式基底で分解でき、 $h(a,b)$ が素イデアルに対応する素数、2,3,5,19 で分解できるものを選定する。表 2 に素イデアルによる篩結果を示す。素イデアルによる篩には、平方剰余の項が必要でこれを 4 個使用する。素イデアル基底の数が 4 個で平方剰余と合わすと 8 個であり、その個数より 5 個多い 13 個の篩結果を得る。素数基底の-1 と一次式基底の $2M+1, 2M+5$ は使用しないため、表 2 から除いた。表 2 中の $B1, B3$ はそれぞれ $M, 2M+3$ に対応する。

表 2 の No.1～No.3 は下記の関係を示す。表 2 の値は各基底の指数を示すため、全てゼロ以上の整数である。

No.1: $M+9 = 176 = 2^4 \cdot 11$, $h(a,b) = abs(2 \cdot 9^2 - 27 \cdot 1^2) = 135 = 3^3 \cdot 5$

No.2: $M+4 = 171 = 3^2 \cdot 19$, $h(a,b) = abs(2 \cdot 4^2 - 27 \cdot 1^2) = 5$

No.3: $M+3 = 170 = 2 \cdot 5 \cdot 17$, $h(a,b) = abs(2 \cdot 3^2 - 27 \cdot 1^2) = 9 = 3^2$

表 2. 素イデアルによる篩結果

No	aM+b の係数		aM+b の分解											h(a,b)の分解			
			素数基底及び一次式基底											素イデアル基底			
	a	b	2	3	5	7	11	13	17	19	23	B1	B3	2	3	5	19
19	1	9	4	0	0	0	1	0	0	0	0	0	0	0	3	1	0
20	1	4	0	2	0	0	0	0	0	1	0	0	0	0	0	1	0
21	1	3	1	0	1	0	0	0	1	0	0	0	0	0	2	0	0
22	1	2	0	0	0	0	0	2	0	0	0	0	0	0	0	0	1
23	1	1	3	1	0	1	0	0	0	0	0	0	0	0	0	2	0
24	1	0	0	0	0	0	0	0	0	0	0	1	0	0	3	0	0
25	1	-2	0	1	1	0	1	0	0	0	0	0	0	0	0	0	1
26	1	-6	0	0	0	1	0	0	0	0	1	0	0	0	2	1	0
27	2	9	0	0	0	3	0	0	0	0	0	0	0	1	3	0	0
28	2	3	0	0	0	0	0	0	0	0	0	0	1	1	2	1	0
29	2	-9	0	0	2	0	0	1	0	0	0	0	0	1	3	0	0
30	3	11	0	9	0	0	0	0	0	0	0	0	0	0	0	0	0
31	3	-11	0	1	0	1	2	0	0	0	0	0	0	0	0	0	0

従属行の決定のための行列作成のため、平方剰余として、4 個の素数 23,29,43,47 にそれぞれ対応する値(23,5),(29,12),(43,11),(47,15)を使用する。

5. 従属行の決定

(1) 従属行計算行列

表 1 及び表 2 を合わせたものに対し、18 個の基底(素数、一次式と素イデアル)と 4 個の平方剰余に対応する部分の 2 の剰余から、下記の行列(31×22 次元)が作成される。

	素数基底	一次式	イデアル	平方剰余	
	0 0 1 1 1 0 0 1 0 0	1 0 0 0	0 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 1 1 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 0 0 0 0	0 1 0 0	0 0 0 0	0 0 0 0	
	0 1 1 0 1 0 0 0 0 0	0 1 0 0	0 0 0 0	0 0 0 0	
	1 0 1 1 1 1 0 1 0 0	0 1 0 0	0 0 0 0	0 0 0 0	
	0 1 0 1 0 0 0 1 1 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 1 0	0 0 0 0	0 0 0 0	
	0 1 1 1 0 1 0 0 1 0	0 0 0 0	0 0 0 0	0 0 0 0	
	0 0 0 1 1 1 0 0 0 0	0 0 0 1	0 0 0 0	0 0 0 0	← 10 行
	0 1 1 1 0 1 0 0 0 1	0 0 0 1	0 0 0 0	0 0 0 0	
	1 1 0 0 0 0 0 1 0 0	0 0 0 1	0 0 0 0	0 0 0 0	
A =	1 0 1 1 1 0 0 1 0 1	0 0 1 0	0 0 0 0	0 0 0 0	
	0 1 0 1 1 0 0 1 0 0	1 0 0 0	0 0 0 0	0 0 0 0	

1 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 1 1 1 0 0 1　0 0 0 0　0 0 0 0　0 0 0 0
1 0 0 0 0 1 1 0 1 0　0 0 0 0　0 0 0 0　0 0 0 0
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 1 1 0　0 1 0 1
0 0 0 0 0 0 0 0 1 0　0 0 0 0　0 0 1 0　1 1 0 0 ← 20 行
0 1 0 1 0 0 0 1 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 1　1 1 1 0
0 1 1 0 1 0 0 0 0 0　0 0 0 0　0 0 0 0　1 1 1 1
0 0 0 0 0 0 0 0 0 0　1 0 0 0　0 1 0 0　0 1 1 0
0 0 1 1 0 1 0 0 0 0　0 0 0 0　0 0 0 1　0 1 1 1
0 0 0 0 1 0 0 0 0 1　0 0 0 0　0 0 1 0　0 1 1 1
0 0 0 0 1 0 0 0 0 0　0 0 0 0　1 1 0 0　1 1 1 1
0 0 0 0 0 0 0 0 0 0　0 0 1 0　1 0 1 0　0 1 0 1
0 0 0 0 0 0 1 0 0 0　0 0 0 0　1 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　1 0 0 1 ← 30 行
0 1 0 1 0 0 0 0 0 0　0 0 0 0　0 0 0 0　1 1 1 1

(2) 行列消去

単位行列をEとする、行列Aの右にEを追加して行列AをEと合わせて消去する。

行列Aの下三角部分が総てゼロとなるEの消去結果を下記に示す。

この最後の 11 行が従属となる行列の行番号を示す。

消去後のE

行　| 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 2 3 3 <-- 列番号(10)
番号 | 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 <-- 列番号(1)

21　| 0 0 0 1 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
22　| 0 1 1 0 0 0 0 0 0 0 1 1 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
23　| 0 1 0 0 0 0 0 1 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
24　| 1 1 0 0 1 1 1 1 0 1 0 1 0 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0 0 0 0
25　| 0 1 1 0 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
26　| 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 0 0
27　| 1 1 0 0 0 0 0 0 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
28　| 0 1 1 0 1 1 0 1 0 1 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 1 0 0 0
29　| 0 1 1 0 1 1 1 1 0 1 0 1 0 0 0 1 0 0 0 1 1 0 1 0 0 1 1 0 1 0 0
30　| 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 1 0
31　| 1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1

(3) 従属行

行列消去し、行列Aが全てゼロになった行のEの行で非ゼロとなる列が従属行を示す。

従って、従属行は 11 組あり次のようになる。

(a) 従属行 1 ： 4, 6, 10, 12

(b) 従属行 2 ： 2, 3, 11, 12, 16, 18

(c) 従属行 3 ： 2, 8, 11, 12, 13

(d) 従属行 4 ： 1, 2, 5, 6, 7, 8, 10, 12, 19, 20, 23, 24

(e) 従属行 5 ： 2, 3, 7, 8, 11, 12, 16, 17

(f) 従属行 6 ： 1, 3, 14

(g) 従属行 7 ： 1, 2, 11, 12, 15

(h) 従属行 8 ： 2, 3, 5, 6, 8, 10, 12, 19, 23, 27, 28

(i) 従属行 9 ： 2, 3, 5, 6, 7, 8, 10, 12, 16, 20, 21, 23, 26, 27, 29

(j) 従属行 10 ： 1, 2, 21, 30

(k) 従属行 11 ： 1, 7, 8, 9, 23, 31

7. イデアルの平方根

従属行 4,8,9,10,11 は素イデアル篩の結果を含んでいるため、イデアルの平方根 $H_k(M)$ を求める必要がある。これらから作成される関数 $F_k(\theta)$ は下記の様になる。

従属行 4: $F_4(\theta) = (\theta+9)(\theta+4)(\theta+1)\theta$

従属行 8: $F_8(\theta) = (\theta+9)(\theta+1)(2\theta+9)(2\theta+3)$

従属行 9: $F_9(\theta) = (\theta+4)(\theta+3)(\theta+1)(\theta-6)(2\theta+9)(2\theta-9)$

従属行 10: $F_{10}(\theta) = (\theta+3)(3\theta+11)$

従属行 11: $F_{11}(\theta) = (\theta+1)(3\theta-11)$

$f(\theta) = 2\theta^2 - 27,\ f(M) \equiv 0 \pmod N$ の関係を使用し、$H_k(M) = F_k(\theta)^{1/2}$ を求める。

これは、直接求まらないので、下記のようにして求める。ここで、m は $F_k(\theta)$ を作成する、θ の一次式の数である。

$$2 \cdot B_k(\theta)^2 \equiv 2^{m-1} F_k(\theta) \pmod{f(\theta)}$$

から $B_k(\theta)$ を非線形連立一次方程式を解き求める。次に下記で $H_k(M)$ を求める。

$$H_k(M) \equiv B_k(M) \cdot D^{(m-2)/2} \pmod N, \quad D \equiv 1/2 \equiv 27876 \pmod N$$

具体的に計算すると下記のようになる。

従属行 4: $2^3 \cdot F_4(\theta) \equiv 1800\theta + 6750,\ B_4(\theta) \equiv 10\theta + 45,\ H_4(M) \equiv 27018$

従属行 8: $2^3 \cdot F_8(\theta) \equiv 10800\theta + 40500,\ B_8(\theta) \equiv 30\theta + 90,\ H_8(M) \equiv 2550$

従属行 9: $2^5 \cdot F_9(\theta) \equiv 64800\theta + 243000,\ B_9(\theta) \equiv 60\theta + 270,\ H_9(M) \equiv 25303$

従属行 10: $2 \cdot F_{10}(\theta) \equiv 40\theta + 147$、これを満たす $B_{10}(\theta)$ は存在しない。

従属行 11: $2 \cdot F_{11}(\theta) \equiv -16\theta + 59,\ B_{11}(\theta) \equiv \theta - 4,\ H_{11}(M) \equiv 163$

6. 因数分解

(1) 従属行 1: 4,6,10,12

表 1 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(3 \cdot 13^2 \cdot 335 \cdot 339)^2 \equiv (2^4 \cdot 7^2 \cdot 17)^2 \pmod{55751}$

計算すると下記のようになる。

$13328^2 \equiv 13328^2 \pmod{55751}$

これは自明解のため分解できない。

(2) 従属行 2: 2,3,11, 2,16, 8

表 1 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(2^4 \cdot 5^3 \cdot 11 \cdot 13 \cdot 167 \cdot 339)^2 \equiv (7 \cdot 19 \cdot 23)^2 \pmod{55751}$

計算すると下記のようになる。

$1078^2 \equiv 3059^2 \pmod{55751}$

従って下記のようになる。

GCD(3059-1078,55751)=283, GCD(3059+1078,55751)=197

即ち、55751=197·283 となる。

(3) 従属行 3: 2,8,11,12,13

同様に、下記が成立する。

$16961^2 \equiv 19^2 \pmod{55751}$

従って、55751=197·283 となる。

(4) 従属行 4: 1,2,5,6,7,8,10,12,19,20,23,24

イデアルの平方根が 27018 である。

よって、下記が成立する。

$3579^2 \equiv 21413^2 \cdot 27018^2 \equiv 8307^2 \pmod{55751}$

従って、55751=197·283 となる。

(5) 従属行 5: 2,3,7,8,11,12,16,17

同様に、下記が成立する。

$3234^2 \equiv 9177^2$

従って、55751=197·283 となる。

(6) 従属行 6: 1,3,14

同様に、下記が成立する。

$27^2 \equiv 27^2 \pmod{55751}$

これは自明解のため分解できない。

(7) 従属行 7: 1,2,11,12,15

同様に、下記が成立する。

$16961^2 \equiv 19^2 \pmod{55751}$

従って、55751=197·283 となる。

(8) 従属行 8: 2,3,5,6,8,10,12,19,23,27,28

イデアルの平方根が 27018 である。

よって、下記が成立する。

$14220^2 \equiv 7429^2 \cdot 2550^2 \equiv 11390^2 \pmod{55751}$

従って、55751=197·283 となる。

(9) 従属行 9：2,3,5,6,7,8,10,12,16,20,21,23,26,27,29

イデアルの平方根が 27018 である。

よって、下記が成立する。

$5908^2 \equiv 437^2 \cdot 25303^2 \equiv 18713^2 \pmod{55751}$

従って、55751=197·283 となる。

(10) 従属行 10：1,2,21,30

イデアルの平方根が求まらない。

よって、分解できない。

(11) 従属行 11：1,7,8,9,23,31

イデアルの平方根が 163 である。

よって、下記が成立する。

$16841^2 \equiv 171^2 \cdot 163^2 \equiv 27873^2 \pmod{55751}$

従って、55751=197·283 となる。