3 次多項式篩法(P3S)による因数分解例

2006/4/7 後 保範(早稲田大学)

1. 概要

(1) 3 次多項式篩法

合成数 N に対して 3 次関数 $f(x)$ を使用して篩を行い、因数分解する。

$f(x)=Ax^3+Bx^2+D,\ f(M)=0 \bmod N$ に対して、

$g(x)=(A_1x+a)(A_2x+b)(A_3x+c)-f(x)$

$A_1A_2A_3=A,\ A_2A_3a+A_1A_3b+A_1A_2c=B$

となる $g(M)$ を作成し、a,b を動かして $g(M)$ 素数基底で因数分解する。

このとき、$g(M)=sM+abc-D$ と表し、s を下記で求める。

(2) 関数の形

(a) $A=1$

条件： $a+b+c=B$

$s=ab+bc+ca$

(b) A が 1 以外の素数

条件： $A_1=A,\ \ a+A(b+c)=B$

$s=ab+ac+Abc$

(c) $A=A_1A_2$

条件： $A_1A_2=A,\ \ A_2a+A_1b+A_1A_2c=B$

$s=ab+A_2ac+A_1bc$

(d) $A=A_1A_2A_3$

条件： $A_1A_2A_3=A,\ \ A_2A_3a+A_1A_3b+A_1A_2c=B$

$s=A_3ab+A_2ac+A_1bc$

2. 計算対象

$N=5917147$ を多項式篩法で因数分解する。

篩には下記の多項式 $f_1(x)$, $f_2(x)$, $f_3(x)$ を使用する。

多項式の選定は 3 次と 2 次の係数(A,B)が小さく、D が負でその絶対値が 5000 以下のものとした。

$f_1(x)=3x^3+4x^2-4728,\ \ f_1(125)=N$

$f_2(x)=5x^3-3x^2-4225,\ \ f_2(106)=N$

$f_3(x)=6x^3-8x^2-2853,\ \ f_2(100)=N$

素数基底は-1 と 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71 の 20

個の素数を使用する。

3. 多項式ふるい

(1) $f_1(x) = 3x^3 + 4x^2 - 4728$ による篩

$$g(x) = (3x+a)(x+b)(x+c) - f_1(x) = sx + abc + 4728$$

$$s = a(b+c) + 3bc$$

M=125, a+3(b+c)=4 で $g(M)$ が素数基底により分解できるものを表 1 に示す。

表 1. $f_1(x)$ による篩結果

NO	係数 a, b, c の値			s, g(M)の値		g(M)の分解結果
	a	b	c	s	g(M)	
1	-14	6	0	-84	-5772	$-2^2*3*13*37$
2	-14	3	3	-57	-2523	$-3*29^2$
3	-11	6	-1	-73	-4331	-61*71
4	-11	3	2	-37	37	37
5	-8	5	-1	-47	-1107	-3^3*41
6	-8	4	0	-32	728	2^3*7*13
7	-8	3	1	-23	1829	31*59
8	-8	2	2	-20	2196	2^2*3^2*61
9	-5	6	-3	-69	-3807	-3^4*47
10	-5	5	-2	-45	-847	$-7*11^2$
11	1	4	-3	-35	341	11*31
12	1	3	-2	-17	2597	7^2*53
13	7	3	-4	-43	-731	-17*43
14	10	2	-4	-44	-852	-2^2*3*71
15	10	1	-3	-29	1073	29*37
16	10	-1	-1	-17	2613	3*13*67
17	13	0	-3	-39	-147	$-3*7^2$
18	13	-1	-2	-33	629	17*37
19	16	-2	-2	-52	-1708	-2^2*7*61

表 1 の中で 3M+a, M+b, M+c のいずれもが素数基底で分解されるものを直接分解と言う。一方、3M+a, M+b, M+c の中の 1 個又は 2 個は素数基底で分解されないが、分解されないものが複数発生し消去できるものを組合せ分解と言う。

直接分解できるもの関係式を表 2 に示す。表 2 中の NO は表 1 中の該当 NO である。そのままの関係式は $2^2*3*5^2*13*37*41=-7*11^2$ の様に両辺ともに平方数にならないが、左辺が平方数になるように調整し、$(2*3*5*13*37*41)^2=-3*7*11^2*13*37*41$ の様に変形している。

表 2. 直接分解による関係式($f_1(x)$)

表 1 対応 NO	関係式
2	$(2^7*19)^2 = -3*29^2$
10	$(2*3*5*13*37*41)^2 = -3*7*11^2*13*37*41$
11	$(2^2*3*43*47*61)^2 = 3*11*31*43*47*61$
12	$(2^5*3*41*47)^2 = 3*7^2*41*47*53$
15	$(2*3*5*7*11*31)^2 = 5*11*29*37*61$
16	$(2^2*5*7*11*31)^2 = 3*5*7*11*13*67$
19	$(3*17*23*41)^2 = -2^2*7*17*23*61$

直接分解できないが、組み合わせると分解できるもの関係式を表 3 に示す。表 3 中の NO は表 1 中の該当 NO である。この場合も、そのままでは両辺とも平方数にならないので、左辺が平方数になるように変更している。

表 3. 組合せ分解による関係式($f_1(x)$)

表 1 対応 NO	関係式
1, 9	$(2*5^2*19*37*61*131)^2 = 2^2*5^2*13*37^2*47*61$
3, 9	$(2^3*5*7*13*31*37*61*131)^2 = 3^4*5*7*13*31*37*47*61^2*71$
5, 8	$(2^2*5*13*31*127*367)^2 = -2^3*3^5*5*13*31*41*61$
6, 8	$(3*5^2*43*127*367)^2 = 2^5*3^3*5*7*13*43*61$
7, 8	$(2^4*3*7*127*367)^2 = 2^2*3^2*7*31*59*61$
4, 14	$(2^5*5*7*11^2*13*127)^2 = -2^3*3*5*11*13*37*71$
17, 18	$(2^4*3*5^2*31*41*61*97)^2 = -2*3^2*5*7^2*17*31*37*41*61$

(2) $f_2(x) = 5x^3 - 3x^2 - 4225$ による篩

$g(x) = (5x+a)(x+b)(x+c) - f_2(x) = sx + abc + 4225$

$s = a(b+c) + 5bc$

M=106, a+5(b+c)=-3 で $g(M)$ が素数基底により分解できるものを表 4 に示す。

表 4. $f_2(x)$ による篩結果

NO	係数 a, b, c の値			s, g(M)の値		g(M)の分解結果
	a	b	c	s	g(M)	
1	-18	2	1	-44	-475	-5^2*19
2	-13	3	-1	-41	-82	-2*41
3	-8	3	-2	-38	245	$5*7^2$
4	-3	3	-3	-45	-518	-2*7*37
5	-3	1	-1	-5	3698	$2*43^2$
6	-3	0	0	0	4225	5^2*13^2
7	2	4	-5	-102	-6627	$-3*47^2$
8	17	-1	-3	-53	-1342	-2*11*61
9	17	-2	-2	-48	-795	-3*5*53
10	22	-2	-3	-80	-4123	-7*19*31

表 4 の中で、5M+a, M+b, M+c が素数基底で直接分解できるもの関係式を表 5 に示す。表 5 中の NO は表 4 中の該当 NO である。表 5 の関係式は左辺が平方数になるように調整してある。

表 5. 直接分解による関係式($f_2(x)$)

表 4 対応 NO	関係式
6	$(2*17*31*53)^2 = 5^2*13^2*17*31$

表 4 の中で、5M+a, M+b, M+c が素数基底では直接分解できないが、組み合わせると分解できるものの関係式を表 6 に示す。表 6 中の NO は表 4 中の該当 NO である。表 6 の関係式は左辺が平方数になるように調整してある。

表 6. 組合せ分解による関係式($f_2(x)$)

表 4 対応 NO	関係式
1, 5	$(2^6*3^2*5*7*17*31*107)^2 = -2^2*5^3*7*17*19*31*43^2$
2, 3	$(2^2*3^2*5*7*11*13*29*47*109)^2 = -2*3*5^2*7^3*11*13*29*41*47$
3, 4, 11	$(2^5*3^2*13*17*23*29*31*103*109)^2 = 2*3*5*7^4*17*19*23*29*31^2*37$
9, 10, 11	$(2^6*3*5*7*13^2*23*103*547)^2 = -2*3*5^2*7^2*11*13*19*23*31*53*61$

(3) $f_3(x) = 6x^3 - 8x^2 - 2853$ による篩

$$g(x) = 2(3x+a)(x+b)(x+c) - f_3(x) = sx + 2abc + 2853$$

$$s = 2a(b+c) + 6bc$$

M=100, a+3(b+c)=-4 で $g(M)$ が素数基底により分解できるものを表 7 に示す。

表 7. $f_3(x)$ による篩結果

NO	係数 a, b, c の値			s, g(M)の値		g(M)の分解結果
	a	b	c	s	g(M)	
1	-10	2	0	-40	-1147	-31*37
2	-10	1	1	-34	-567	-3^4*7
3	-4	3	-3	-54	-2475	-3^2*5^2*11
4	-4	1	-1	-6	2261	7*17*19
5	-1	3	-4	-70	-4123	-7*19*31
6	-1	0	-1	2	3053	43*71
7	2	3	-5	-98	-7007	$-7^2*11*13$
8	5	0	-3	-30	-147	$-3*7^2$
9	5	-1	-2	-18	1073	29*37
10	8	1	-5	-94	-6627	$-3*47^2$
11	8	-2	-2	-40	-1083	$-3*19^2$

表 7 の中で、3M+a, M+b, M+c が素数基底で直接分解できるもの関係式を表 8 に示す。

表 8 中の NO は表 7 中の該当 NO である。表 8 の関係式は左辺が平方数になるように調整してある。

表 8. 直接分解による関係式($f_3(x)$)

表 7 対応 NO	関係式
1	$(2^3*3*5^2*17*29)^2 = -2*3*5*17*29*31*37$
6	$(2^2*3*5*11*13*23)^2 = 2*11*13*23*43*71$
2	$(2*5*29*101)^2 = -3^4*5*7*29$
9	$(2*3*5*7*11*61)^2 = 5*11*29*37*61$
11	$(2^3*7^3*11)^2 = -2*3*7*11*19^2$

表 7 の中で、3M+a, M+b, M+c が素数基底では直接分解できないが、組み合わせると分解できるものの関係式を表 9 に示す。表 9 中の NO は表 7 中の該当 NO である。表 9 の関係式は左辺が平方数になるように調整してある。

表 9. 組合せ分解による関係式($f_3(x)$)

表 7 対応 NO	関係式
4, 10	$(2^4*3*5*7*11*19*37*101)^2 = -2*3*5*7^2*17*19^2*37*47^2$
3, 5, 8	$(2^7*3*5^2*13*23*37*61*97*103)^2 =$ $-2*3^4*5^3*7^3*11*13*19*23*31*37*61$

4. 従属行の決定

(1) 分解関係行列

表 2, 3, 5, 6, 8, 9 から 26 個の関係式が得られるが、1 個(表 2 の 15 と表 8 の 9)は同一の関係式のため除くと 25 個の関係式が得られる。これに、素数基底を使用して行列にすると表 10 が得られる。表 10 で平方数は左辺の値を計算し、基底素数の数字は、右辺にその因子が何個含まれているかを示したものである。平方数は分解する値(N=5917147)の法の基で成立すればよいので、N での剰余の値である。

表 10. 分解関係行列

	素 数 基 底																				
No	-1	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
1	1	0	1	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0
2	1	0	1	0	1	2	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0
3	0	0	1	0	0	1	0	0	0	0	0	1	0	0	1	1	0	0	1	0	0
4	0	0	1	0	2	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0
5	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0
6	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0
7	1	2	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0
8	0	0	0	2	0	0	2	1	0	0	0	1	0	0	0	0	0	0	0	0	0

9	1	1	1	1	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0
10	0	1	0	0	0	1	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1
11	1	0	4	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
12	1	1	1	0	1	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0
13	0	2	5	0	0	0	1	0	0	0	0	0	2	0	0	1	0	0	1	0	0
14	0	0	4	1	1	0	1	0	0	0	0	1	1	0	0	1	0	0	2	0	1
15	1	3	5	1	0	0	1	0	0	0	0	1	0	1	0	0	0	0	1	0	0
16	0	5	3	1	1	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0
17	0	2	2	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0
18	1	3	1	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1
19	1	1	2	1	2	0	0	1	0	0	0	1	1	1	0	0	0	0	1	0	0
20	1	2	0	3	1	0	0	1	1	0	0	1	0	0	2	0	0	0	0	0	0
21	1	1	1	2	3	1	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0
22	0	1	1	1	4	0	0	1	1	1	1	2	1	0	0	0	0	0	0	0	0
23	1	1	1	2	2	1	1	0	1	1	0	1	0	0	0	0	1	0	1	0	0
24	1	1	1	1	2	0	0	1	2	0	0	0	1	0	0	2	0	0	0	0	0
25	1	1	4	3	3	1	1	0	1	1	0	1	1	0	0	0	0	0	1	0	0

No	平方数	No	平方数	No	平方数	No	平方数	No	平方数
1	2432	6	47740	11	29290	16	2385350	21	5546179
2	591630	7	48093	12	30184	17	3826330	22	2280729
3	1479372	8	55862	13	2777741	18	4809081	23	3430723
4	184992	9	295800	14	2189494	19	959225	24	4445953
5	140910	10	197340	15	2888279	20	710016	25	3783966

(2) 従属行計算行列

表 10 の素数基底に対応する部分の 2 の剰余から下記の行列が作成される。

$$
A = \begin{bmatrix}
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&1&0&0&1&0&0&0&0&0&1&0&0&1&1&0&0&1&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&1&0&1&0&0&0&0&0&1&0&0\\
0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
1&0&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&1&0&0&1&1&1&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&1&0&0&1&0&0&0&0&1&0&0&0&0&0&1\\
1&0&0&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&1&0&0\\
0&0&0&1&1&0&1&0&0&0&0&1&1&0&0&1&0&0&0&0&1\\
1&1&1&1&0&0&1&0&0&0&0&1&0&1&0&0&0&0&1&0&0\\
0&1&1&1&1&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0
\end{bmatrix}
$$

1 1 1 1 0 1 1 0 0 0 0 0 1 0 0 0 0 0 0 0 1
1 1 0 1 0 0 0 1 0 0 0 1 1 1 0 0 0 0 1 0 0
1 0 0 1 1 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0
1 1 1 0 1 1 1 0 0 0 1 0 0 1 0 1 0 0 0 0 0
0 1 1 1 0 0 0 1 1 1 1 0 1 0 0 0 0 0 0 0 0
1 1 1 0 0 1 1 0 1 1 0 1 0 0 0 0 1 0 1 0 0
1 1 1 1 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0
1 1 0 1 1 1 1 0 1 1 0 1 1 0 0 0 0 0 1 0 0

(3) 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 5 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 0 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 <-- 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 <-- 列番号(1)
22	1 1 1 0 0 0 0 1 0 0 1 0 0 0 1 1 0 0 1 0 1 0 0 0 0
22	0 0 0 0 1 0 1 1 0 1 1 0 1 1 0 1 0 0 0 0 0 0 0 0 0
23	0 1 1 1 0 0 1 1 0 0 0 0 0 0 1 1 0 0 1 1 0 0 1 0 0
24	0 0 1 0 1 0 0 1 0 0 1 0 1 0 0 1 0 0 0 0 0 0 0 1 0
25	0 0 1 0 0 0 0 1 1 0 0 0 1 0 1 1 0 0 1 0 0 1 0 0 1

(4) 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５組あり次のようになる。

従属行１： 1, 2, 3, 8, 11, 15, 16, 19, 21
従属行２： 5, 7, 8, 10, 11, 13, 14, 16
従属行３： 2, 3, 4, 7, 8, 15, 16, 19, 20, 23
従属行４： 3, 5, 8, 11, 13, 16, 24
従属行５： 3, 8, 9, 13, 15, 16, 19, 22, 25

5. 因数分解

(1) 従属行１： 1,2,3,8,11,15,16,19,21

表 10 に従属行を当てはめ、N=5917147 を法とすると下記の関係が成立する。

$(2432*191630*1479372*55862*29290*2888279*2385350*959225*5546179)^2$

$= (2^5*3^9*5^4*7^4*11^2*13^3*29^2*31^2*37^2*41*43*47*61^2)^2$

計算すると下記のようになる。

$4599960^2 = 4599960^2 \mod 5917147$

これは自明な関係なので、分解できない。

(2) 従属行２： 5,7,8,10,11,13,14,16

表 10 に従属行を当てはめ、N=5917147 を法とすると下記の関係が成立する。

$(140910*48093*55862*197340*29290*2777741*2189494*2385350)^2$

$= (2^5*3^8*5^3*7^2*11*13^3*17*23*29*31*37^2*43*47*61^3*71)^2$

計算すると下記のようになる。

$1946617^2 = 2739379^2 \mod 5917147$

従って下記のようになる。

GCD(2739379-1946617,5917147) = 3571

GCD(2739379+1946617,5917147) = 1657

これより、5917147 は 1657 と 3571 に分解される。

(3) 従属行３： 2,3,4,7,8,15,16,19,20,23

同様に表 10 に従属行を当てはめ、N=5917147 を法とすると下記の関係が成立する。

$3344445^2 = 2290593^2 \mod 5917147$

従って下記のようになる。

GCD(3344445-2290593,5917147) = 1657

GCD(3344445+2290593,5917147) = 3571

これより、5917147 は 1657 と 3571 に分解される。

(4) 従属行４： 3,5,8,11,13,16,24

同様に表 10 に従属行を当てはめ、N=5917147 を法とすると下記の関係が成立する。

$3344445^2 = 84565^2 \mod 5917147$

従って下記のようになる。

GCD(980886-84565,5917147) = 3571

GCD(980886+84565,5917147) = 1657

これより、5917147 は 1657 と 3571 に分解される。

(5) 従属行５： 3,8,9,13,15,16,19,22,25

同様に表 10 に従属行を当てはめ、N=5917147 を法とすると下記の関係が成立する。

$5423394^2 = 3994994^2 \mod 5917147$

従って下記のようになる。

GCD(5423394-3994994,5917147) = 3571

GCD(5423394+3994994,5917147) = 1657

これより、5917147 は 1657 と 3571 に分解される。