3 次多項式篩法(P3S)による因数分解例

2006/2/28 後 保範(早稲田大学)

2006/3/23　追加、改定

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。

$f(x)=Ax^3+Bx^2+Cx+D,\ f(M)=0 \bmod N$ に対して、B が A の倍数となる整数 A,B,C,D,M を見つける。説明を簡単にするため B を A の倍数にした。

$g(x)=A(x+a)(x+b)(x+c)=Ax^3+A(a+b+c)x^2+A(ab+bc+ca)x+Aabc$

に対して、$A(a+b+c)=B$ の関係を保って整数 a,b,c を選ぶと下記が成立する。

$g(x)=sx+t \bmod f(x),\ \ s=A(ab+bc+ca)-C,\ t=Aabc-D$

従って、$A(M+a)(M+b)(M+c)=sM+t \bmod N$ となる。

そこで、適当な素数による素数基底を使用して、$M+a,M+b,M+c$ 及び $sM+t$ を篩により分解したものを、基底の数以上集める。その後は MPQS と同様である。

この、3 次多項式篩法を P3S(3rd Polynomial Sieve)と名づける。

一般に多項式篩法を PS(Polynomial Sieve)と言う。

(2) GNFS,MPQS と PS の比較

GNFS(一般数体篩法)、MPQS(複数多項式 2 次篩法)と PS(多項式篩法)の性質の比較を表 1 に示す。

表 1. PS,GNFS,MPQS の比較

項目	PS	GNFS	MPQS
使用多項式	2～4 次式	2～7 次式	2 次式
使用多項式の数	多数	1 個	多数
片側が平方数	変形し成立	不成立	成立
一次式の項の分解	多くは不要	必須	不要
平方根の計算	不要	必須	不要
篩分解式の等式	成立	不成立	成立
計算量係数(p)	1/3?	1/3	1/2

計算量 = $O(\exp(c\cdot s^{p}\cdot \ln(s)^{1-p})$

ここで、N は分解対象数で c は定数、$s=\ln(N)$ で p は表 1 に示す係数である。

2. 計算対象

$N=55751$ を多項式篩法で因数分解する。

篩には下記の多項式 $f_1(x)$ と $f_2(x)$ を使用する。

$f_1(x)=x^3+x-15x+5,\ \ f_1(38)=55751$

$f_2(x)=2x^3+2x^2-2x+11,\ \ f_2(30)=55751$

素数基底は-1 と 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 の 14 個の素数を使用する。

3. 多項式篩

(1) $f_1(x)=x^3+x^2-15x+5$ による篩

M=38, A=1, a+b+c=1 で素数基底により分解できるもの。

表 1. $f_1(x)$ による篩結果

係数 a, b, c			係数 s, t			分解結果	
a	b	c	s	t	sM+t	A(M+a)(M+b)(M+c)	sM+t
3	−1	−1	10	−2	378	37^2*41	$2*3^3*7$
3	−4	2	1	−29	9	$2^4*5*17*41$	3^2
5	−5	1	−10	−30	−410	$3^2*11*13*43$	$-1*2*5*41$
5	−4	0	−5	−5	−195	$2^2*17*19*43$	$-1*3*5*13$
5	−3	−1	−2	10	−66	$5*7*37*43$	$-1*2*3*11$
5	−2	−2	−1	15	−23	2^4*3^4*43	$-1*23$
6	−5	0	−15	−5	−575	2^3*3*11^2*19	$-1*5^2*23$
6	−4	−1	−11	19	−399	$2^3*11*17*37$	$-1*3*7*19$
7	−5	−1	−22	30	−806	$3^3*5*11*37$	$-1*2*13*31$
8	−6	−1	−35	43	−1287	$2^6*23*37$	$-1*3^2*11*13$

(2) $f_2(x)=2x^3+2x^2-2x+11$ による篩

M=30, A=2, a+b+c=1 で素数基底により分解できるもの。

表 2. $f_2(x)$ による篩結果

係数 a, b, c			係数 s, t			分解結果	
a	b	c	s	t	sM+t	A(M+a)(M+b)(M+c)	sM+t
1	0	0	2	−11	49	$2^3*3^2*5^2*31$	7^2
3	−1	−1	−8	−5	−245	$2*3*11*29^2$	$-1*5*7^2$
−3	2	2	−14	−35	−455	$2^{11}*3^3$	$-1*5*7*13$
4	−4	1	−30	−43	−943	$2^3*13*17*31$	$-1*23*41$
6	−4	1	−50	37	−1463	$2^4*3^2*13*29$	$-1*7*11*19$
7	−3	−3	−64	115	−1805	$2*3^6*37$	$-1*5*19^2$
−8	2	7	−114	−235	−3655	$2^7*11*37$	$-1*5*17*43$

(3) 一方を二乗の形に変形

sM+t の方が奇数ベキの場合は、両辺にその値を乗算し二乗の形に変形する。

(1) 及び(2)から下記が得られる。

表 3. 篩の変形結果

No.	V	A(M+a)(M+b)(M+c)*V	U=(sM+t)*V	sqrt(U)
1	$2*3*7$	$2*3*7*37^2*41$	$2^2*3^4*7^2$	126
2	1	$2^4*5*17*41$	3^2	3
3	$-1*2*5*41$	$-1*2*3^2*5*11*13*41*43$	$2^2*5^2*41^2$	410
4	$-1*3*5*13$	$-1*2^2*3*5*13*17*19*43$	$3^2*5^2*13^2$	195
5	$-1*2*3*11$	$-1*2*3*5*7*11*37*43$	$2^2*3^2*11^2$	66

6	−1*23	$-1*2^4*3^4*23*43$	23^2	23
7	−1*23	$-1*2^3*3*11^2*19*23$	5^2*23^2	115
8	−1*3*7*19	$-1*2^3*3*7*11*17*19*37$	$3^2*7^2*19^2$	399
9	−1*2*13*31	$-1*2*3^3*5*11*13*31*37$	$2^2*13^2*31^2$	806
10	−1*11*13	$-1*2^6*11*13*23*37$	$3^2*11^2*13^2$	429
11	1	$2^3*3^2*5^2*31$	7^2	7
12	−1*5	$-1*2*3*5*11*29^2$	5^2*7^2	35
13	−1*5*7*13	$-1*2^{11}*3^3*5*7*13$	$5^2*7^2*13^2$	455
14	−1*23*41	$-1*2^3*13*17*23*31*41$	23^2*41^2	943
15	−1*7*11*19	$-1*2^4*3^2*7*11*13*19*29$	$7^2*11^2*19^2$	1463
16	−1*5	$-1*2*3^6*5*37$	5^2*19^2	95
17	−1*5*17*43	$-1*2^7*5*11*17*37*43$	$5^2*17^2*43^2$	3655

4. 従属行の決定

(1) 分解関係行列

表 3 に素数基底を使用して行列にすると次の表が得られる。

表 4. 分解関係行列

	素数基底															平方数
No.	−1	2	3	5	7	11	13	17	19	23	29	31	37	41	43	sqrt(U)
1	0	1	1	0	1	0	0	0	0	0	0	0	2	1	0	126
2	0	4	0	1	0	0	0	1	0	0	0	0	0	1	0	3
3	1	1	2	1	0	1	1	0	0	0	0	0	0	1	1	410
4	1	2	1	1	0	0	1	1	1	0	0	0	0	0	1	195
5	1	1	1	1	1	1	0	0	0	0	0	0	1	0	1	66
6	1	4	4	0	0	0	0	0	0	1	0	0	0	0	1	23
7	1	3	1	0	0	2	0	0	1	1	0	0	0	0	0	115
8	1	3	1	0	1	1	0	1	1	0	0	0	1	0	0	399
9	1	1	3	1	0	1	1	0	0	0	0	1	1	0	0	806
10	1	6	0	0	0	1	1	0	0	1	0	0	1	0	0	429
11	0	3	2	2	0	0	0	0	0	0	0	1	0	0	0	7
12	1	1	1	1	0	1	0	0	0	0	2	0	0	0	0	35
13	1	11	3	1	1	0	1	0	0	0	0	0	0	0	0	455
14	1	3	0	0	0	0	1	1	0	1	0	1	0	1	0	943
15	1	4	2	0	1	1	1	0	1	0	1	0	0	0	0	1463
16	1	1	6	1	0	0	0	0	0	0	0	0	1	0	0	95
17	1	7	0	1	0	1	0	1	0	0	0	0	1	0	1	3655

(2) 従属行計算行列

表 4 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。

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

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

(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とＥの消去結果を下記に示す。

Ａ	Ｅ
1 1 0 1 0 1 1 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 1 1 0 1 0 0 0 0 0 0 0 0 1 0	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 1 0 1 0 1 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 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 0 0 0
0 0 0 0 1 1 0 1 1 0 0 0 0 0 0	1 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 1 0 1 0 1 0 0 1 0 0	1 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 1 0 1 1 0 1 1 0 1	0 1 1 1 0 1 0 0 1 0 0 0 0 0 0 0
0 0 0 0 0 0 0 1 1 0 0 1 1 0 0	1 0 1 1 1 1 0 0 1 1 0 0 0 0 0 0
0 0 0 0 0 0 0 0 1 0 0 0 0 1 1	0 1 0 0 1 0 0 1 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 1 0 0 1 1 1	1 1 1 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 0	0 1 1 1 1 1 0 0 0 1 0 0 0 0 1 0
0 0 0 0 0 0 0 0 0 0 0 0 1 0 1	1 1 0 0 0 1 1 1 0 0 0 1 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 1 0	0 0 1 0 0 1 0 0 0 1 0 0 0 0 0 1
Ｅの列番号-->	1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 0 1 1 0 0 1 1 1 0 0 0 1 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 0 1 0 1 0 0 0 1 0 1 1 0 0 0 0 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 1 0 0 1 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 1 0 0 1 0 0 1 0 0 0 0 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４組あり次のようになる。

従属行１： 2, 4, 5, 8, 9, 10, 14

従属行２： 1, 3, 5, 9, 11, 12

従属行３： 5, 6, 10, 13

従属行４： 4, 7, 10, 17

5. 因数分解

(1) 従属行１：2, 4, 5, 8, 9, 10, 14

表 4 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。

$(3*195*66*399*804*429*943)^2 = (2^{10}*3^3*5^2*7*11^2*13^2*17^2*19*23*31*37^2*41*43)^2$

計算すると下記のようになる。

$2393^2 = 2984^2 \mod 55751$

従って下記のようになる。

$(2984-2393)(2984+2393) = 591*5377 = 3*197*19*283 = 0 \mod 55751$

これより、55751 は 197 と 283 に分解される。

(2) 従属行２： 1, 3, 5, 9, 11, 12

表 4 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。

$(126*410*66*806*7*35)^2 = (2^4*3^5*5^3*7*11^2*13*29*31*37^2*41*43)^2$

計算すると下記のようになる。

$2709^2 = 15120^2 \mod 55751$

従って下記のようになる。

$(15120-2709)(15120+2709) = 12411*17829 = 63*197*63*283 = 0 \mod 55751$

これより、55751 は 197 と 283 に分解される。

(3) 従属行３： 5, 6, 10, 13

同様に行うと下記の関係になる。

$10555^2 = 10555^2 \mod 55751$

これは自明な関係なので、分解できない。

(4) 従属行４： 4, 7, 10, 17

同様に行うと下記の関係になる。

$20673^2 = 20673^2 \mod 55751$

これは自明な関係なので、分解できない。

6. 高速化方法

(1) a を固定し、$g(M) \bmod f(M)$ を使用した分解

a を固定し $B = As,\ a+b+c = s$ とすると、$g(b)$ は下記のように x になる。

$$
\begin{aligned}
g(M) &= \left(A(ab+bc+ca)-C\right)M + Aabc - D \\
&= \left(A(-b^2+(s-a)b+(s-a)a)-C\right)M + Aa(s-a)b - Aab^2 - D \\
&= \alpha b^2 + \beta b + \gamma
\end{aligned}
$$

$\alpha = -A(M+a),\ \beta = A(s-a)(M+a),\ \gamma = \big(Aa(s-a)-C\big)M - D$

従って、a を固定した素数基底 p による分解は、$g(b) = 0 \bmod p$ となる b を利用する。素数 p のベキ乗も利用する。

(a) 具体例 1

$f_1(x) = x^3 + x^2 - 15x + 5,\ f_1(38) = 55751$ に適用する。

$a = 5$ に固定し、$A = 1,\ M = 38,\ s = 1,\ C = -15,\ D = 5$ で $\alpha = -43, \beta = -172,$ $\gamma = -195$ となる。即ち、$g(M) = -43b^2 - 172b - 195 = -43(b+2)^2 - 23$ となる。

従って、下記の様になる。$p = 29,31,43$ は b が存在しないので省略。

表 5. $a = 5$ で $g(M) = 0 \bmod p$ となる b の値

p	2	3	5	7	11	13	17	19	23	37	41	3^2	5^2
b	1	0	0	--	-1	0	--	--	-2	6	1	2	6
	--	-1	1	--	-3	-4	--	--	--	-10	-5	3	-10

表 5 を使用すると、$b = -5 \sim 10$ までの p の因子は下記のようになる。

表 6. $a = 5$ のとき $g(M)$ の素数基底による分解

	基底素数(p)										累計	g(M)	因子
b	2	3	3^2	5	5^2	11	13	23	37	41	T	g	g/T
-5	2	1	1	5	1	1	1	1	1	41	410	-410	-1
-4	1	3	1	5	1	1	13	1	1	1	195	-195	-1
-3	2	3	1	1	1	11	1	1	1	1	66	-66	-1
-2	1	1	1	1	1	1	1	23	1	1	23	-23	-1
-1	2	3	1	1	1	11	1	1	1	1	66	-66	-1
0	1	3	1	5	1	1	13	1	1	1	195	-195	-1
1	2	1	1	5	1	1	1	1	1	41	410	-410	-1
2	1	3	3	1	1	1	1	1	1	1	9	-711	-79
3	2	3	3	1	1	1	1	1	1	1	18	-1098	-61
4	1	1	1	1	1	1	1	1	1	1	1	-1571	- -
5	2	3	1	5	5	1	1	1	1	1	30	-2130	-71
6	1	3	1	5	1	1	1	1	37	1	2775	-2775	-1
7	2	1	1	1	1	1	1	1	1	1	2	-3506	- -
8	1	3	1	1	1	11	1	1	1	1	33	-4323	-131
9	2	3	1	1	1	1	13	1	1	1	78	-5226	-67
10	1	1	1	5	1	11	1	1	1	1	55	-6215	-113

b=-2 で対称のため、b=-5, -4, -3 はそれぞれ b=1, 0, -1 と同じ結果となる。

(2) M+a の共通因子利用

(M+a)(M+b)(M+c)と分解するため、(M+a), (M+b), (M+c)は同じ値が複数発生する。

そのため、基底因子で分解できなくてもよい。

3 次式による多項式篩では g(b)の高速な分解が最も重要となる。

7. 計算量の評価

(1) 計算量の評価方法

3 次多項式篩(P3S)と GNFS(一般数体篩)、MPQS(複数多項式２次篩)の計算量の比較評価を行う。計算量は分解すべき関数 g(x)の大きさにより評価する。

分解すべき関数 g(x)の大きさのを基本に、同時に分解する必要な値も考慮して、評価関数 h(x)を定め、その大きさで評価する。

(a) 分解すべき関数 g(x)の大きさ

因数分解する合成数を N、篩の上限を d とすると g(x)は下記で近似される。

P3S ： $g(x) = d^2N^{1/3}$

GNFS： $g(x) = d^kN^{1/(k+1)}$, k は多項式の次数

MPQS： $g(x) = dN^{1/2}$

(b) 評価関数 h(x)の大きさ

3 次多項式篩(P3S)で $M=N^{1/3}$ とすると(M+a),(M+b),(M+c)で a,b,c は d と同程度の値も同時に分解する必要があるが、同じ値が多数発生し共用できるために、この項の分解が必要なものはほとんどなく、増加分は $M^{1/10}$ 程度とする。

k 次多項式の GNFS は $M=N^{1/(k+1)}$ とすると a,b は d と同程度の値で、a+bM を g(x)と同時に分解する必要があり、共用はできないので負担が大きく、増加分は $M^{1/2}$ 程度とする。

一方、MPQS は g(x)と同時に分解するものがなく、各方式の評価関数 h(x)の大きさは下記のようになる。

P3S ： $h(x) = M^{1/10}d^2N^{1/3} = d^2N^{11/30}$

GNFS： $h(x) = M^{1/2}d^kN^{1/(k+1)} = d^kN^{3/2(k+1)}$ ， k は多項式の次数

MPQS： $h(x) = dN^{1/2}$

(2) 具体的な評価関数 h(x)の大きさ

N が 10 進 30,50,100,150,200,250,300 桁のときの h(x)の 10 進桁数で評価する。

表 7 に各方式の評価関数 h(x)の 10 進桁数を示す。

値が小さいほど計算量が少ないことをします。目安として、値が 2 大きいと計算量は約 2 倍である。

表 7. P3S,GNFS,MPQS の評価関数 h(x)の桁数比較

解法	多項式次数	N	30	50	100	150	200	250	300
		d	3	4	5	6	7	8	9
P3S	3	h(x)	17	26	47	67	87	108	128
GNFS	3	h(x)	23	35	58	80	103	126	149
	4	h(x)	24	35	55	75	95	115	135
	5	h(x)	26	37	55	74	92	111	129
	6	h(x)	27	39	56	74	92	110	127
MPQS	2	h(x)	18	29	55	81	107	133	159
比率(倍)	(対MPQS)	PS	0.94	0.90	0.85	0.83	0.81	0.81	0.81
		MPQS	1.28	1.21	1.00	0.91	0.86	0.83	0.80

この表から、N が 100 桁の近くで GNFS と MPQS が交差することが分かる。
また、30 桁～250 桁位の範囲では P3S(3 次多項式篩)が演算量は一番少ないと予測される。

図 1 に各方式の評価関数 h(x)の 10 進桁数のグラフを示す。
GNFS(3),GNFS(6)はそれぞれ 3 次の GNFS 及び 6 次の GNFS を示す。

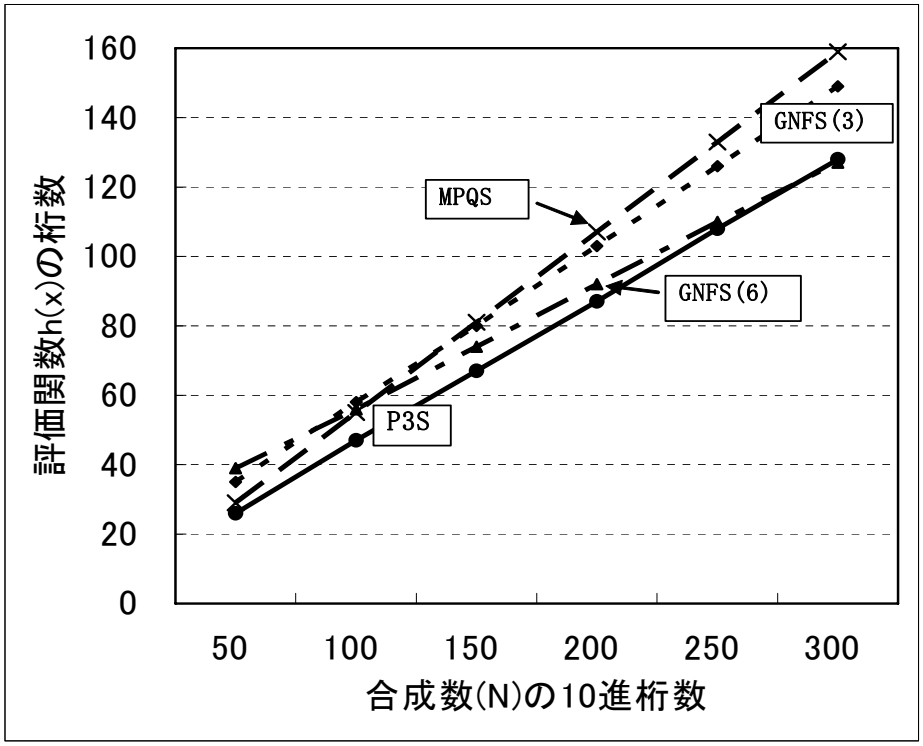

図 1. P3S,GNFS,MPQS の評価関数 h(x)の桁数比較グラフ