

RSA暗号計算 No.6

MBPS(多重基底多項式ふるい法)

2007年5月

後 保範 (東京工芸大学)

目次

1. MBPSの概要
2. 2次のDBPSによるふるい
3. 2次のDBPSによる因数分解
4. DBPSによるふるい例
5. DBPSによる因数分解例

1. MBPSの概要

MBPS (Multiple Base Polynomial Sieve)
のアイデアー

$$QS : (x+k)^2 \equiv s \cdot x + t \pmod{n}$$

$s \cdot x + t$ を素数基底で分解

$$MBPS: (x+a)(x+b) - f(x) = v(s \cdot x + t), f(M) = n$$

$x+a, x+b, s \cdot x + t$ を素数基底で分解
及び共通一次式の取出し

1.1 MBPSの種類

- (1) DBPS(2重基底多項式ふるい法)
 - (a) $f(x)$ は2次多項式→ここで説明
 - (b) $f(x)$ は3次多項式
 - (c) より高速化したもの → DBPS2
- (2) TBPS(3重基底多項式ふるい法)
DBPSにGNFSの素イデアル分解の方法を取り入れた方式
(2次式、3次式及びTBPS2)がある

2. 2次のDBPSによるふるい

2次のDBPSによるふるいの手順

- (1) 2次関数 $f(x)=Ax^2+Bx+C$ と $M(f(M)=n)$ の選定
- (2) 素数基底の選定と a, b の範囲決定
- (3) $A_1 \cdot M+a, A_2 \cdot M+b$ を素数基底で分解し、分解できた、 a, b をふるいに採用。ここで、 $A_1 \cdot A_2=A$ とする。
- (4) $A_1 \cdot M+a, A_2 \cdot M+b$ が分解できなく、 $|a|, |b|$ が小さいものを指定個数だけ1次基底に採用
- (5) $g(x)=(A_1 \cdot x+a)(A_2 \cdot x+b)-f(x)=v \cdot (s \cdot x+t)$ から s, t を計算してふるいをおこなう。(素数基底+1次式基底)の数より採用データ数を多くする
- (6) ふるいで採用したデータで行列を作成

2.1 2次関数の選定

$$f(x) = Ax^2 + Bx + C \text{ で}$$

$f(M) \equiv 0 \pmod{n}$, n は分解対象数を定める。ここで、 A, B, C 及び M は整数。
そのとき、下記のようにする。

- (a) $|A|+|B|+|C|$ をできるだけ小さく
- (b) ほぼ同じ桁数の整数 A_1, A_2 を使用し
 A は $A=A_1 \cdot A_2$ と分解できる。

2.2 素数基底の選定

素数基底は下記により選定する

- (1) 指定値以下の素数を総て選定
- (2) -1も素数基底に加える

<理由>

$g(x)=(A_1 \cdot x+a)(A_2 \cdot x+b)-f(x)=v \cdot (s \cdot x+t)$
とするととき、 $A_1 \cdot M+a$, $A_2 \cdot M+b$, $s \cdot M+t$ は
正の整数であるが v は負の値を含む
整数となるため。

2.3 A_1M+a, A_2M+b の素数基底分解

- (1) 整数 a, b の範囲を決める
- (2) $A_1 \cdot M+a$ 及び $A_2 \cdot M+b$ を素数基底で分解する。
- (3) 分解された、 $A_1 \cdot M+a$ 及び $A_2 \cdot M+b$ はふるいのために保存する。
- (4) 分解されないものは、1次式基底の候補に入れる。

2.4 1次式基底の選定

- (1) $A_1 \cdot M + a$ 及び $A_2 \cdot M + b$ が素数基底で分解されず、1次式基底候補に入ったものの中で $|a|, |b|$ の値が指定以下のもの。
- (2) $g(x) = (A_1 \cdot x + a)(A_2 \cdot x + b) - f(x) = v \cdot (s \cdot x + t)$ でふるいを行い、同一の $s \cdot x + t$ で、 v が異なり、かつ $s \cdot x + t$ が素数基底で分解されないもの。

2.5 $g(x)=v(sx+t)$ 計算によるふるい

- (1) 選定した $A_1 \cdot x+a, A_2 \cdot x+b$ を使用し下記で整数 v, s, t を計算。ただし、 s は正又はゼロ

$$g(x)=(A_1 \cdot x+a)(A_2 \cdot x+b)=v \cdot (s \cdot x+t)$$

- (2) $s, |t|$ が指定値以下なら下記を行う。
- (a) $s \cdot x+t$ が1次式基底なら採用
 - (b) $s \cdot M+t$ が素数基底で分解できれば採用
 - (c) 同一の $s \cdot x+t$ が複数次(v は異なる)なら採用

2.6 ふるい結果の行列作成

- (1) 採択したデータが、素数基底+1次式基底の合計数以上になれば行列を作成
- (2) 各データに毎に下記項目の値を入れる
 - (a) a,bの値
 - (b) 素数基底の各素数のベキ数
 - (c) 1次式基底の各1次式のベキ数
- (3) 各素数と各1次式に対応するベキ数は $A_1 \cdot x + a, A_2 \cdot x + b$ なら正、 $v \cdot (s \cdot x + t)$ なら負

3. DBPSによる因数分解

ふるい結果の行列による因数分解

- (1) 0-1行列の作成
- (2) 行列消去による従属行の算出
- (3) 従属行から $\alpha^2 \equiv \beta^2 \pmod{n}$ 算出
- (4) $\text{GCD}(|\alpha - \beta|, n)$ を計算し、
nを因数分解

4. DBPSによるふるい例

計算対象

$n = 55751$ が分解対象数

$$f(x) = 2x^2 - 27$$

$$f(M) \equiv 0 \pmod{n}, M=167$$

$$(2x+a) \cdot (x+b) - f(x) = v \cdot (s \cdot x + t)$$

4.1 使用する基底因子

(1) 素数基底: P

23までの素数と-1の10個

$$P = \{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23\}$$

(2) 1次式基底: B (素数基底で分解不可)

M+b及び2M+aより5個選ぶ

$$B = \{M-3, M, 2M+1, 2M+3, 2M+5\}$$

4.2 ふるいの基本式

$$f(x) = 2x^2 - 27$$

$$g(x) = (2x+a)(x+b) - f(x)$$

$$= S \cdot x + T = v \cdot (s \cdot x + t)$$

$$S = a + 2b, \quad T = a \cdot b + 27$$

$$v = \text{GCD}(|S|, |T|) \cdot \text{sign}(S)$$

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

4.3 $(2x+a), (x+b)$ の選定

- (1) $|a|, |b|$ がともに9以下を対象
- (2) $2M+a, M+b$ が素数基底Pで分解

$$a = \{-9, -4, -2, 2, 4, 6, 8, 9\}$$

$$b = \{-7, -6, -5, -2, 1, 2, 3, 4, 8, 9\}$$

- (3) 1次式基底

$$B1=M-3=164, B2=M=167, B3=2M+1=235$$

$$B4=2M+3=237, B5=2M+5=239$$

4.4 ふるいの方針

- (1) ふるいの基本式により該当する a, b から v, s, t を計算

$$g(x) = (2x+a)(x+b) - f(x) = v \cdot (s \cdot x + t)$$

- (2) $|s|$ が9以下ならふるい候補に入れる
- (3) $s \cdot x + t$ が1次式基底に一致するか、 $s \cdot M + t$ が素数基底で分解されたら採用(篩結果NO.に番号を入れる)

4.5 ふるいの過程(1/4)

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	$3(2M+9)=3 \cdot 7^3$	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	$-3(2M-9)=-3 \cdot 5^2 \cdot 13$	4
8	1	4	9	31	1534		
9	1	3	7	30	1199		
10	1	2	5	29	864	$2^5 \cdot 3^3$	5
11	1	1	3	28	529	23^2	6
12	1	0	1	27	194		
13	1	-2	-3	25	-476	$-2^2 \cdot 7 \cdot 17$	7
14	1	-3	-5	24	-811		
15	1	-5	-9	22	-1481		

4.5 ふるいの過程(2/4)

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	$9(M+4)=3^4 \cdot 19$	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

4.5 ふるいの過程(3/4)

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		

4.5 ふるいの過程(4/4)

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		

4.6 ふるい結果の行列(1/2)

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

4.6 ふるい結果の行列(2/2)

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

5. DBPSによる因数分解例

ふるい結果の行列による因数分解

- (1) 0-1行列の作成
- (2) 行列消去による従属行の算出
- (3) 従属行から $\alpha^2 \equiv \beta^2 \pmod{n}$ 算出
- (4) $\text{GCD}(|\alpha - \beta|, n)$ を計算し、
n を因数分解

5.2 消去した行列

行 番号	0000000001111111111222 : 列番号(10)	1234567890123456789012 : 列番号(1)
14	0000101000010100000000	: 従属行1
15	0100101011011010000000	
16	0100101010011001000000	
17	0100101011011000100000	
18	1100101011011000010000	
19	1100101000011000001000	
20	001100001100000000100	
21	010110110101100000010	
22	010110101101100000001	: 従属行9

各行の1がある列番号が従属行となる

5.3 従属行一覽

- (1) 従属行1: 5, 7, 12, 14
- (2) 従属行2: 2, 5, 7, 9, 10, 12, 13, 15
- (3) 従属行3: 2, 5, 7, 9, 12, 13, 16
- (4) 従属行4: 1, 3, 17
- (5) 従属行5: 1, 2, 5, 7, 9, 10, 12, 13, 18
- (6) 従属行6: 1, 2, 5, 7, 12, 13, 19
- (7) 従属行7: 3, 4, 9, 10, 20
- (8) 従属行8: 2, 4, 5, 7, 8, 10, 12, 13, 21
- (9) 従属行9: 2, 4, 5, 7, 9, 10, 12, 13, 22

5.4 従属行1の $\alpha^2 \equiv \beta^2$ の計算

ふるい結果の行列の5,7,12,14行の素数基底及び1次式基底で等式を作成する。

このとき、 $B1=164, B2=167, B3=335, B4=337, B5=339$ である。

左辺は正のベキ、右辺は負のベキを集める。

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

$$\text{即ち、} 13328^2 \equiv 13328^2 \pmod{55751}$$

5.5 各従属行の $\alpha^2 \equiv \beta^2$

- (1) $13328^2 \equiv 13328^2 \pmod{55751}$: 自明解
- (2) $24042^2 \equiv 11024^2 \pmod{55751}$
- (3) $11477^2 \equiv 1824^2 \pmod{55751}$
- (4) $27^2 \equiv 27^2 \pmod{55751}$: 自明解
- (5) $24042^2 \equiv 11024^2 \pmod{55751}$
- (6) $11477^2 \equiv 1824^2 \pmod{55751}$
- (7) $13041^2 \equiv 13041^2 \pmod{55751}$: 自明解
- (8) $24042^2 \equiv 11204^2 \pmod{55751}$
- (9) $24042^2 \equiv 13041^2 \pmod{55751}$

5.6 因数分解結果

自明解でないものだけ

$$(1)(5)(8)(9) : 24042^2 \equiv 11024^2 \pmod{55751}$$

$$\text{GCD}(|24042-11024|, 55751) = 283$$

→ $55751 = 283 \times 197$ と因数分解

$$(3)(6) : 11477^2 \equiv 1824^2 \pmod{55751}$$

$$\text{GCD}(|11477-1824|, 55751) = 197$$

→ $55751 = 197 \times 283$ と因数分解