RSA暗号計算 No.5

GNFS(一般数体ふるい法)

2007年5月

後　保範　(東京工芸大学)

目次

1. GNFS(一般数体ふるい法)の概要
2. SNFS(特殊数体ふるい法)とGNFS
3. GNFSによるふるい
4. 代数平方根の計算
5. GNFSによる因数分解
6. GNFSによるふるい例
7. GNFSによる因数分解例

1. GNFS(一般数体ふるい法)の概要

(1) $f(x)=Ax^3+Bx^2+Cx+D$; d次多項式

$f(M)\equiv 0 \pmod n$, n ; 分解対象数

(2) a_k, b_kは下記を共に満たす整数

$$\prod (a_k+b_k \cdot M) = (\prod p_j^{sj}) \equiv \alpha^2 \pmod n$$

$$\prod (a_k+b_k \cdot x) \equiv Q(x) \equiv q(x)^2 \pmod{f(x)}$$

$$q(M) \equiv \beta \pmod n, \ p_j\text{は素数}$$

(3) $\alpha^2 \equiv \beta^2 \pmod n$ → nを因数分解

1.1 GNFSの理論背景(1/2)

(1) $\prod(a_k+b_k.x) \equiv Q(x) \equiv q(x)^2 \pmod{f(x)}$

を満たす多項式q(x)の存在

→ SNFSの考えを一部変更

SNFS: 生成元が2乗になるように選ぶ

q(x)が生成元から直接求められる

GNFS: 生成元は求められない

→ 素イデアルと平方剰余を2乗になるように選ぶ

q(x)は直接求められない

1.2 GNFSの理論背景(2/2)

(2) 代数平方根の計算

$Q(x) \equiv q(x)^2 \pmod{f(x)}$

の関係から$q(x)$を求める。

(a) s,aは整数、nは合成数で$s^2 \equiv a \pmod{n}$

→ sを計算はnの分解とほぼ同等（困難)

(b) xの多項式$q(x)^2 \equiv Q(x) \pmod{f(x)}$

→ $q(x)$は計算できる

2. SNFSとGNFS

SNFS(特殊数体ふるい法)

(1) $f(x)=x^5+1$のように特定の形 $(f(M)=n)$

(2) ふるい(素数基底と生成元)

(a) $a_k+b_k \cdot M$を素数基底で分解のものを選ぶ

(b) $a_k+b_k \cdot \theta$ が生成元で分解のものを選ぶ

(3) $\alpha^2 \equiv \beta^2 \pmod n$を作成

$\alpha \leftarrow a_k+b_k \cdot M, \quad \beta \leftarrow a_k+b_k \cdot \theta$

(4) $\mathrm{GCD}(|\alpha-\beta|,n)$でnの因数分解

2.1 SNFSとGNFSの違い(1/2)

(1) 多項式

SNFS: 特殊な形のd次多項式だけ

GNFS: 総ての形のd次多項式

(2) イデアル$(a+b\cdot\theta)$の分解

SNFS: 生成元で分解

GNFS: 素イデアルQ(p:s)で分解

Q(p:s) : $f(s)\equiv 0 \pmod p$, pは素数

Q(p:s)で分解 : $N(a,b)=|b^d f(-a/b)|$がpで分解

2.2 SNFSとGNFSの違い(2/2)

(3) $\prod(a_k+b_k\cdot\theta)\equiv Q(\theta)\equiv q(\theta)^2 \bmod (f(\theta))$

SNFS : 生成元から$q(\theta)$を直接計算

各生成元を偶数乗になるよう選定

GNFS: 生成元は使用できない

→ 各素イデアルを偶数乗にし、更に

平方剰余で$q(\theta)$の存在率を上げる

→ $Q(\theta)\equiv q(\theta)^2 \bmod (f(\theta))$の関係

を利用し、代数平方根$q(\theta)$を計算

3. GNFSによるふるい

計算手順

(1) $f(M) \equiv 0 \pmod n$となる多項式$f(x)$を求める

(2) 基底(素数P,素イデアルQ)選定

(3) $a_k + b_k \cdot M$がPで分解されるものを選定

(4) $a_k + b_k \cdot \theta$がQで分解されるものを選定

(5) (3)(4)で共に選定されたものに対し平方剰余Rを計算する

(6) (P+Q+R)の要素数より少し多く選定する

3.1 多項式の算出

(1) 多項式の次数d(3～7)を決める

分解桁数が多くなるとdを大きくする

(2) 多項式の係数を決める

$f(x) = A_d x^d + \ldots + A_1 x + A_0$

$f(M) \equiv 0 \pmod{n}$, nは分解対象数

を満足し、$|A_d|+\ldots+|A_1|+|A_0|$ができるだけ小さくなるように決める

3.2 基底の選定

(1) 素数基底: P

指定数以下の素数を総て選ぶ

(2) 素イデアル基底: Q

指定数以下の素数pに対して

$s^2 \equiv n \pmod{p}$, nは分解対象数

となる整数sが存在するp,sの組Q(p:s)を

総て選ぶ

3.3 素数基底でのふるい

(1) 互いに素な整数a,bに対して下記を行う

ただし、$|a|<M_a$, $0<b|<M_b$とする

(2) 各a,bに対して$T(a,b)=1$とする

(3) 各bと基底内の各素数pの正べキp^sに対して

$a_0+b\cdot M\equiv 0 \pmod{p^s}$なる$a_0$を選ぶ

$|a_0+k\cdot p^s|<M_b$となる総ての整数kに対して

$T(a_0+k\cdot p^s,b) = T(a_0+k\cdot p^s,b) \times p^s$ を計算

(4) $T(a,b)=a+b\cdot M$となれば、(a,b)を選定

3.4 素イデアル基底でのふるい(1/2)

ふるいの方針

f(x)はf(M)≡0 (mod n)となるd次の多項式

(1) $N(a+b\cdot\theta) = |b^d \cdot f(-a/b)|$を素イデアル基底Q(p:s)の素数pで分解するものを選ぶ

(2) 「素イデアルQ(p:s)において、a+b·sが素数pで割れるなら、$N(a+b\cdot\theta)$ が素数pで割れる」を利用し高速化

3.4 素イデアル基底でのふるい(2/2)

ふるいの手順

(1) 素数基底で選ばれた$a+b\cdot\theta$を対象

(2) 素イデアルQ(p:s)の素数pで$a+b\cdot s$が割れるかのテストを行う

(3) 該当したQ(p:s)に対して、$N(a+b\cdot\theta)$がpのベキ$p^s(s=1,2\ldots)$で割れるかテスト

(4) $N(a+b\cdot\theta)$がQ(p:s)で割り切れたら選定

3.5 平方剰余の計算

(1) 目的

$$\prod(a_k+b_k\cdot\theta)=Q(\theta)\equiv q(\theta)^2 \pmod{f(\theta)}$$

となるq(θ)の存在確率を高める。

(2) 計算方法

(a) 素イデアル基底より大きい素数に対して、同一方法で平方剰余基底R(p:s)作成

(b) 各行列データに対し、平方剰余を計算

$$\text{平方剰余} = (a - b\cdot s)^{(p-1)/2} \pmod{p}$$

3.6 行列データの作成

行列作成の方法

(1) 素数基底P及び素イデアル基底Qで共に分解された(a,b)を使用する

(2) a,bの値、各素数基底Pの指数ベキ、各素イデアル基底Qの指数ベキを格納

(3) 各データに対し、各平方剰余基底Rに対応する平方剰余(0 or 1)を格納

4. 代数平方根の計算

GNFSにおける代数平方根の計算方法

(1) 選定された従属行(k)よりQ(θ)を計算

$$Q(\theta) \equiv \prod (a_k + b_k \cdot \theta) \pmod{f(\theta)}$$

(2) $Q(\theta) \equiv q(\theta)^2 \pmod{f(\theta)}$の関係から非線形連立方程式を導出

(3) 非線形連立方程式の整数解(q(θ))を求め、$q(M) \pmod{n}$を計算する

4.1 非線形連立方程式の算出(1/2)

$f(x)=x^3+Ax^2+Bx+C$, $f(M)\equiv 0 \pmod n$とし

$$Q(\theta) = a\theta^2 + b\theta + c,\ q(\theta) = x_1\theta^2 + x_2\theta + x_3$$

とする、$Q(\theta) \equiv q(\theta)^2$ から次が得られる

$$q(\theta)^2 - Q(\theta) \equiv g_1(x_1,x_2,x_3)\cdot\theta^2 + g_2(x_1,x_2,x_3)\cdot\theta + g_3(x_1,x_2,x_3) \equiv 0 \pmod{f(\theta)}$$

常に成立には、$g_1\equiv g_2\equiv g_3\equiv 0 \pmod{f(\theta)}$

4.1 非線形連立方程式の算出(2/2)

従って下記の非線形連立方程式が得られる

$$g_1(x_1,x_2,x_3) = (A^2 - B)x_1^2 - 2Ax_1x_2 + x_2^2 + 2x_1x_3 - a = 0$$

$$g_2(x_1,x_2,x_3) = (AB - C)x_1^2 - 2Bx_1x_2 + 2x_2x_3 - b = 0$$

$$g_2(x_1,x_2,x_3) = ACx_1^2 - 2Cx_1x_2 + x_3^2 - c = 0$$

4.2 非線形連立方程式の求解

$G(x)=0$の解$x=(x_1,x_2,x_3)^T$の計算方法

擬似ニュートン法で下記を反復計算する

$$J(x^{(k)})\cdot\Delta x = G(x)^{(k)}$$

$$x^{(k+1)} = x^{(k)} - \Delta x$$

ここで、$G(x)=(g_1(x),g_2(x),g_3(x))^T$で

$$J(x)=\begin{pmatrix} \partial g_1/\partial x_1 & \partial g_1/\partial x_2 & \partial g_1/\partial x_3 \\ \partial g_2/\partial x_1 & \partial g_2/\partial x_2 & \partial g_2/\partial x_3 \\ \partial g_3/\partial x_1 & \partial g_3/\partial x_2 & \partial g_3/\partial x_3 \end{pmatrix}$$

5. GNFSによる因数分解

各従属行を使用して因数分解する

(1) 代数平方根の計算($\beta^2 = q(M)^2$)

(2) 素数基底の平方根の計算

$$\alpha^2 \equiv (\prod p_k^{sk})^2 \pmod{n}$$

(3) (1),(2)から$\alpha^2 \equiv \beta^2 \pmod{n}$

(4) GCD($|\alpha - \beta|$, n)の計算

6. GNFSによるふるい例

(1) 分解対象数

$n = 1333$

(2) 使用多項式

$f(x) = x^3 + 2$

$M = 11, \quad f(M) = n$

(3) GNFSによりふるいを行い、行列データを作成する

6.1 基底の選定

(1) 素数基底P

P = {2,3,5,7,11,13,17,19} : 19までの素数

(2) 素イデアル基底Q (q(p:s))

f(s)≡0 (mod p), pは23までの素数

Qは上記整数sが存在する下記の6個

$q_1(2:0)$, $q_2(3:1)$, $q_3(5:2)$, $q_4(11:4)$,

$q_5(17:8)$, $q_6(23:7)$

6.2 a+b·Mのふるい

素数ふるいの方法

(1) 素数基底Pでa+b·Mを分解する

(2) aは-8～8,bは1～5の範囲の整数で、
aとbは互いに素のものを選ぶ

(3) M=11

(4) Pは{2,3,5,7,11,13,17,19}の8個

6.2 a+b·Mのふるい結果(1/4)

係数		関数値	素数基底								累計	因子
			2	3	5	7	11	13	17	19	T	a+bM /T
a	b	a+bM	P1	P2	P3	P4	P5	P6	P7	P8		
-8	1	3	1	3	1	1	1	1	1	1	3	1
-7	1	4	2^2	1	1	1	1	1	1	1	4	1
-6	1	5	1	1	5	1	1	1	1	1	5	1
-5	1	6	2	3	1	1	1	1	1	1	6	1
-4	1	7	1	1	1	7	1	1	1	1	7	1
-3	1	8	2^3	1	1	1	1	1	1	1	8	1
-2	1	9	1	3^2	1	1	1	1	1	1	9	1
-1	1	10	2	1	5	1	1	1	1	1	10	1
0	1	11	1	1	1	1	11	1	1	1	11	1
1	1	12	2^2	3	1	1	1	1	1	1	12	1
2	1	13	1	1	1	1	1	13	1	1	13	1
3	1	14	2	1	1	7	1	1	1	1	14	1
4	1	15	1	3	5	1	1	1	1	1	15	1

6.2 a+b·Mのふるい結果(2/4)

4	1	15	1	3	5	1	1	1	1	1	15	1
5	1	16	2^4	1	1	1	1	1	1	1	16	1
6	1	17	1	1	1	1	1	1	17	1	17	1
7	1	18	2	3^2	1	1	1	1	1	1	18	1
8	1	19	1	1	1	1	1	1	1	19	19	1
-7	2	15	1	3	5	1	1	1	1	1	15	1
-5	2	17	1	1	1	1	1	1	17	1	17	1
-3	2	19	1	1	1	1	1	1	1	19	19	1
-1	2	21	1	3	1	7	1	1	1	1	21	1
1	2	23	1	1	1	1	1	1	1	1	1	23
3	2	25	1	1	5^2	1	1	1	1	1	25	1
5	2	27	1	3^3	1	1	1	1	1	1	27	1
7	2	29	1	1	1	1	1	1	1	1	1	29
-8	3	25	1	1	5^2	1	1	1	1	1	25	1
-7	3	26	2	1	1	1	1	13	1	1	26	1
-5	3	28	2^2	1	1	7	1	1	1	1	28	1

6.2 a+b·Mのふるい結果(3/4)

-4	3	29	1	1	1	1	1	1	1	1	1	29
-2	3	31	1	1	1	1	1	1	1	1	1	31
1	3	32	2^5	1	1	1	1	1	1	1	32	1
1	3	34	2	1	1	1	1	1	17	1	34	1
2	3	35	1	1	5	7	1	1	1	1	35	1
4	3	37	1	1	1	1	1	1	1	1	1	37
5	3	38	2	1	1	1	1	1	1	19	38	1
7	3	40	2^3	1	5	1	1	1	1	1	40	1
8	3	41	1	1	1	1	1	1	1	1	1	41
-7	4	37	1	1	1	1	1	1	1	1	1	37
-5	4	39	1	3	1	1	1	13	1	1	39	1
-3	4	41	1	1	1	1	1	1	1	1	1	41
-1	4	43	1	1	1	1	1	1	1	1	1	43
1	4	45	1	3^2	5	1	1	1	1	1	45	1
3	4	47	1	1	1	1	1	1	1	1	1	47
5	4	49	1	1	1	7^2	1	1	1	1	49	1

6.2 a+b·Mのふるい結果(4/4)

7	4	51	1	3	1	1	1	1	17	1	51	1
-8	5	47	1	1	1	1	1	1	1	1	1	47
-7	5	48	2^4	3	1	1	1	1	1	1	48	1
-6	5	49	1	1	1	7^2	1	1	1	1	49	1
-4	5	51	1	3	1	1	1	1	17	1	51	1
-3	5	52	2^2	1	1	1	1	13	1	1	52	1
-2	5	53	1	1	1	1	1	1	1	1	1	53
-1	5	54	2	3^3	1	1	1	1	1	1	54	1
1	5	56	2^3	1	1	7	1	1	1	1	56	1
2	5	57	1	3	1	1	1	1	1	19	57	1
3	5	58	2	1	1	1	1	1	1	1	2	29
4	5	59	1	1	1	1	1	1	1	1	1	59
6	5	61	1	1	1	1	1	1	1	1	1	61
7	5	62	2	1	1	1	1	1	1	1	2	31
8	5	63	1	3^2	1	7	1	1	1	1	63	1

6.3 a+b·θのふるい

素イデアルふるいの方法

(1) 素数ふるいで得られたa+bθを対象

(2) 素イデアルQ(p:s)で分解

(a) a+b·sがpで割れるものを探す

(b) a+b·sに対し当該のpのベキ数を探す

N(a,b)がpのベキで割れるかテスト

(3) N(a,b)がpで分解できるものを選択

6.3 a+b·θのふるい結果(1/5)

係数		有効	ノルム		素イデアル基底						累計	因子
			N(a,b)		Q1	Q2	Q3	Q4	Q5	Q6		
a	b	Y		p	2	3	5	11	17	23	T	N(a,b)/T
				s	0	1	2	4	-8	7		
-8	1	1	514		2	1	1	1	1	1	2	257
-7	1	1	345		1	3	5	1	1	23	345	1
-6	1	1	218		2	1	1	1	1	1	2	109
-5	1	1	127		1	1	1	1	1	1	1	127
-4	1	1	66		2	3	1	11	1	1	66	1
-3	1	1	29		1	1	1	1	1	1	1	29
-2	1	1	10		2	1	5	1	1	1	10	1
-1	1	1	3		1	3	1	1	1	1	3	1
0	1	1	2		2	1	1	1	1	1	2	1

6.3 a+b·θのふるい結果(2/5)

1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	6	2	3	1	1	1	1	6	1
3	1	1	25	1	1	25	1	1	1	25	1
4	1	1	62	2	1	1	1	1	1	2	31
5	1	1	123	1	3	1	1	1	1	3	41
6	1	1	214	2	1	1	1	1	1	2	107
7	1	1	341	1	1	1	11	1	1	11	31
8	1	1	510	2	3	5	1	17	1	510	1
-7	2	1	359	1	1	1	1	1	1	1	359
-5	2	1	141	1	3	1	1	1	1	3	47
-3	2	1	43	1	1	1	1	1	1	1	43
-1	2	1	17	1	1	1	1	17	1	17	1
1	2	0	15	1	3	5	1	1	1	0	0

6.3 a+b·θのふるい結果(3/5)

3	2	1	11	1	1	1	11	1	1	11	1
5	2	1	109	1	1	1	1	1	1	1	109
7	2	0	327	1	3	1	1	1	1	0	0
-8	3	1	566	2	1	1	1	1	1	2	283
-7	3	1	397	1	1	1	1	1	1	1	397
-5	3	1	179	1	1	1	1	1	1	1	179
-4	3	0	118	2	1	1	1	1	1	0	0
-2	3	0	62	2	1	1	1	1	1	0	0
-1	3	1	55	1	1	5	11	1	1	55	1
1	3	1	53	1	1	1	1	1	1	1	53
2	3	1	46	2	1	1	1	1	23	46	1
4	3	0	10	2	1	5	1	1	1	0	0
5	3	1	71	1	1	1	1	1	1	1	71

6.3 a+b·θのふるい結果(4/5)

7	3	1	289	1	1	1	1	17^2	1	289	1
8	3	0	458	2	1	1	1	1	1	0	0
-7	4	0	471	1	3	1	1	1	1	0	0
-5	4	1	253	1	1	1	11	1	23	253	1
-3	4	0	155	1	1	5	1	1	1	0	0
-1	4	0	129	1	3	1	1	1	1	0	0
1	4	1	127	1	1	1	1	1	1	1	127
3	4	0	101	1	1	1	1	1	1	0	0
5	4	1	3	1	3	1	1	1	1	3	1
7	4	1	215	1	1	5	1	1	1	5	43
-8	5	0	762	2	3	1	1	1	1	0	0
-7	5	1	593	1	1	1	1	1	1	1	593
-6	5	1	466	2	1	1	1	1	1	2	233

6.3 a+b·θのふるい結果(5/5)

-4	5	1	314	2	1	1	1	1	1	2	157
-3	5	1	277	1	1	1	1	1	1	1	277
-2	5	0	258	2	3	1	1	1	1	0	0
-1	5	1	251	1	1	1	1	1	1	1	251
1	5	1	249	1	3	1	1	1	1	3	83
2	5	1	242	2	1	1	11^2	1	1	242	1
3	5	0	223	1	1	1	1	1	1	0	0
4	5	0	186	2	3	1	1	1	1	0	0
6	5	0	34	2	1	1	1	17	1	0	0
7	5	0	93	1	3	1	1	1	1	0	0
8	5	1	262	2	1	1	1	1	1	2	131

6.4 ふるい結果の行列作成

行列作成の方法

(1) $a+b\cdot\theta$ のふるい結果でN(a,b)/Tが1のものを選択

(2) a,bの係数、素数基底(P)、及び素イデアル基底(Q)のベキ数を取り出す

(3) 各データに対し、素数29及び31に対応する平方剰余(R)を計算し、追加

6.4 ふるい結果の行列

No	a	b	P1	P2	P3	P4	P5	P6	P7	P8	Q1	Q2	Q3	Q4	Q5	Q6	R1	R2
1	-7	1	2	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0
2	-4	1	0	0	0	1	0	0	0	0	1	1	0	1	0	0	0	1
3	-2	1	0	2	0	0	0	0	0	0	1	0	1	0	0	0	0	0
4	-1	1	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1
5	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
6	1	1	2	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0
7	2	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0
8	3	1	1	0	0	1	0	0	0	0	0	0	2	0	0	0	0	0
9	8	1	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	1
10	-1	2	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1
11	3	2	0	0	2	0	0	0	0	0	0	0	0	1	0	0	1	1
12	-1	3	5	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
13	2	3	0	0	1	1	0	0	0	0	1	0	0	0	0	1	0	1
14	7	3	3	0	1	0	0	0	0	0	0	0	0	0	2	0	1	0
15	-5	4	0	1	0	0	0	1	0	0	0	0	0	1	0	1	1	1
16	5	4	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	0
17	2	5	0	1	0	0	0	0	0	1	1	0	0	2	0	0	0	1

7. GNFSによる因数分解例

因数分解の方法

(1) ふるい行列から0-1行列作成

(2) 0-1行列を消去し、従属行の取出し

(3) 各従属行の代数平方根の計算

(4) 各従属行で $\alpha^2 \equiv \beta^2 \pmod{n}$ 計算

(5) $\mathrm{GCD}(|\alpha - \beta|, n)$ を計算し、
nを因数分解

7.1 0-1行列の作成

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

7.2 行列消去し従属行列の取出し

消去された15,16,17行を示す

```
      1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7
    ---------------------------------------
15  |  1 0 1 0 0 1 1 0 0 0 1 0 0 0 1 0 0
16  |  0 1 1 1 0 0 0 1 0 0 0 1 0 1 0 0 0
17  |  0 0 0 0 0 0 0 1 1 1 1 1 0 0 0 1 1
```

これから従属行は下記となる

従属行1 : 1,3,6,7,1,15,　従属行2 : 2,3,4,8,12,14

従属行3 : 8,9,10,11,12,16,17

7.3 代数平方根の計算(1/3)

従属行1 (1,3,6,7,11,15)より

$$F(\theta)=(\theta-7)(\theta-2)(\theta+1)(\theta+2)(2\theta+3)(4\theta-5)$$

$$=529\theta^2-74\theta-908 \mod f(\theta)$$

従って、下記の連立一次方程式が成立する

$$g_1(x) = x_2^2 + 2x_1x_2 - 529 = 0$$

$$g_2(x) = -2x_1^2 + 2x_2x_3 + 74 = 0$$

$$g_3(x) = -4x_1x_2 + x_3^2 + 908 = 0$$

7.3 代数平方根の計算(2/3)

この方程式の整数解は

$x_1=11,\ x_2=21,\ x_3=4$

となり下記が成立する

$$F(\theta)^{1/2} \equiv B(\theta) \equiv 11\theta^2 + 21\theta + 4 \mod f(\theta)$$

$$B(11) \equiv 233 \mod 1333$$

7.3 代数平方根の計算(3/3)

まとめると下記のようになる

従属行1: $B(11) \equiv 233 \pmod{1333}$

従属行2: $B(11) \equiv 608 \pmod{1333}$

従属行3: $B(11) \equiv 1112 \pmod{1333}$

7.4 $\alpha^2 \equiv \beta^2 \pmod n$の計算(1/2)

従属行1 (1,3,6,7,11,15)より素数基底のベキは

$$\alpha^2 \equiv (2^2 \cdot 3^2 \cdot 5 \cdot 13)^2 \equiv 1007^2 \pmod{1333}$$

代数平方根の結果より

$$\beta^2 \equiv B(11)^2 \equiv 233^2 \pmod{1333}$$

従って$\alpha^2 \equiv \beta^2$を適用すると下記となる

$$1007^2 \equiv 233^2 \pmod{1333}$$

7.4 $\alpha^2 \equiv \beta^2 \pmod{n}$の計算(2/2)

まとめると下記のようになる

従属行1 : $1007^2 \equiv 233^2 \pmod{1333}$

従属行2 : $694^2 \equiv 608^2 \pmod{1333}$

従属行3 : $1081^2 \equiv 1112^2 \pmod{1333}$

7.5 GCDを求め、因数分解

(1) 従属行1

GCD(|1007 - 233|,1333) = 43

従って、1333 = 31 × 43

(2) 従属行2

GCD(|694 - 608|,1333) = 43

従って、1333 = 31 × 43

(3) 従属行3

GCD(|1112 - 1081|,1333) = 31

従って、1333 = 31 × 43