RSA暗号解読向け0-1行列の直接解法 (必要理由に変更)

2016年6月9日

後 保範(神奈川大学)

1. はじめに

- 現ネット社会は暗号(公開鍵:RSA)で成立
- 現在GNFS(1次式+多項式)が最速(強度評価)

  疎行列(非ゼロ数/行=数百)→ 0-1行列反復解法

  ふるいと線形計算の時間比は9:1
- 2次式+多項式のGNFSが実現できそう

  現GNFSより係数が小で、ふるい高速化

  非ゼロ数/行=(数百→数百万)→ 0-1行列直接解法

  → 発表を2次式+多項式のGNFS概要

2. 現在の暗号(ハイブリッド)

(1) 公開鍵暗号方式 → 共通鍵の送付

公開鍵で暗号化、秘密鍵で復号化

秘密鍵の送付不要だが遅い

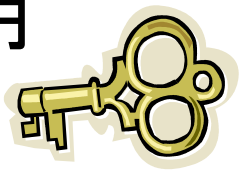
RSA暗号：多数桁数因数分解の難しさを利用

鍵2個

(2) 共通鍵暗号方式 → 本文の送付

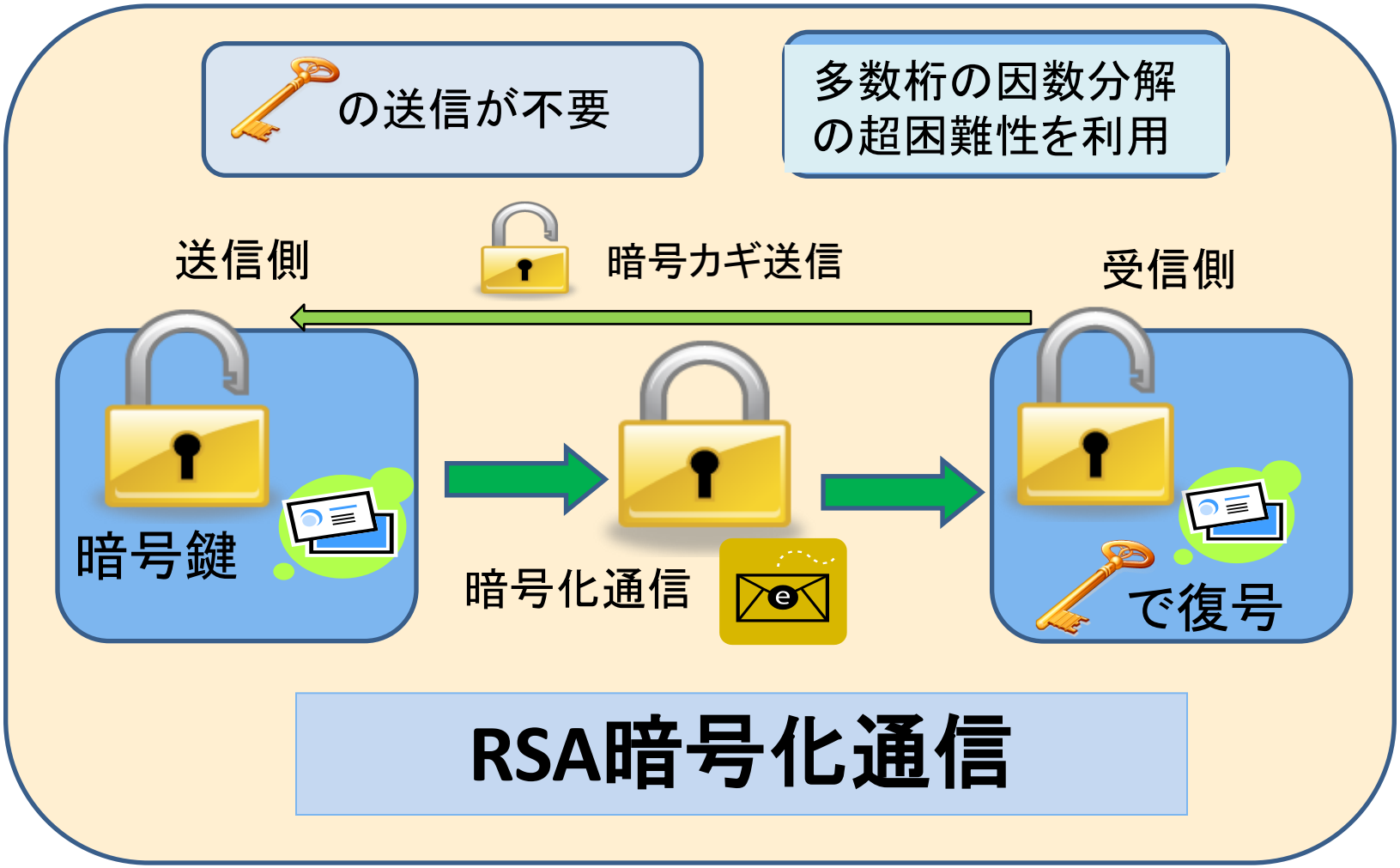
暗号化と復号化で共通の秘密鍵を使用

代表暗号例：AES, RC4(Netscape)



鍵1個

2. RSA暗号とは


の送信が不要
多数桁の因数分解
の超困難性を利用
送信側
暗号カギ送信
受信側
暗号鍵
暗号化通信
で復号
RSA暗号化通信

2. RSA暗号の原理

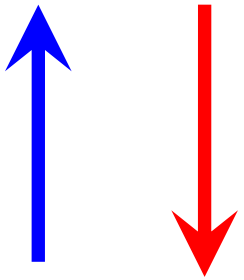
1024ビット(309桁)

104020825032019040734592469269989892952069437280567608281162303008155662346881375166006145095484690073181120801002008117284398265073951835839124365852238489496041645216071420486302806551764597271236680277169585662585060682785083907795107933150484467446870950521704322329021315163976651164626600290991175427177

乗算： 数千回 / s

暗号化、復号化:

数十回 / s ： PC



因数分解(解読)

数年：スパコン

156505591702911312312934897542336100462589397637499374745061303569581122941951458658466588096006025692937083518893745436362413308018973842821873100856446 17 x

664646060886296425367851677122466088330766375237126209727286497601290902458234488921382706457331046487153031722486963900929508400607301572291891914517968 1

3. RSA暗号解読法の推移

- MPQS(複数多項式2次ふるい法） ---①

  QSの改良。QS: $(X+k)^2 - N$を素数分解、$X=[N^{1/2}]$

- GNFS(一般数体ふるい法), Nは分解対象数

  n(5～7)次多項式f(x), f(M)=0 (mod N)を使用

  (1) $|a^n f(-b/a)|$とaM+bを基底(素数)で分解 ---②

  (2) 1次式Ax+B, AM+B=0 (mod N)追加 ---③

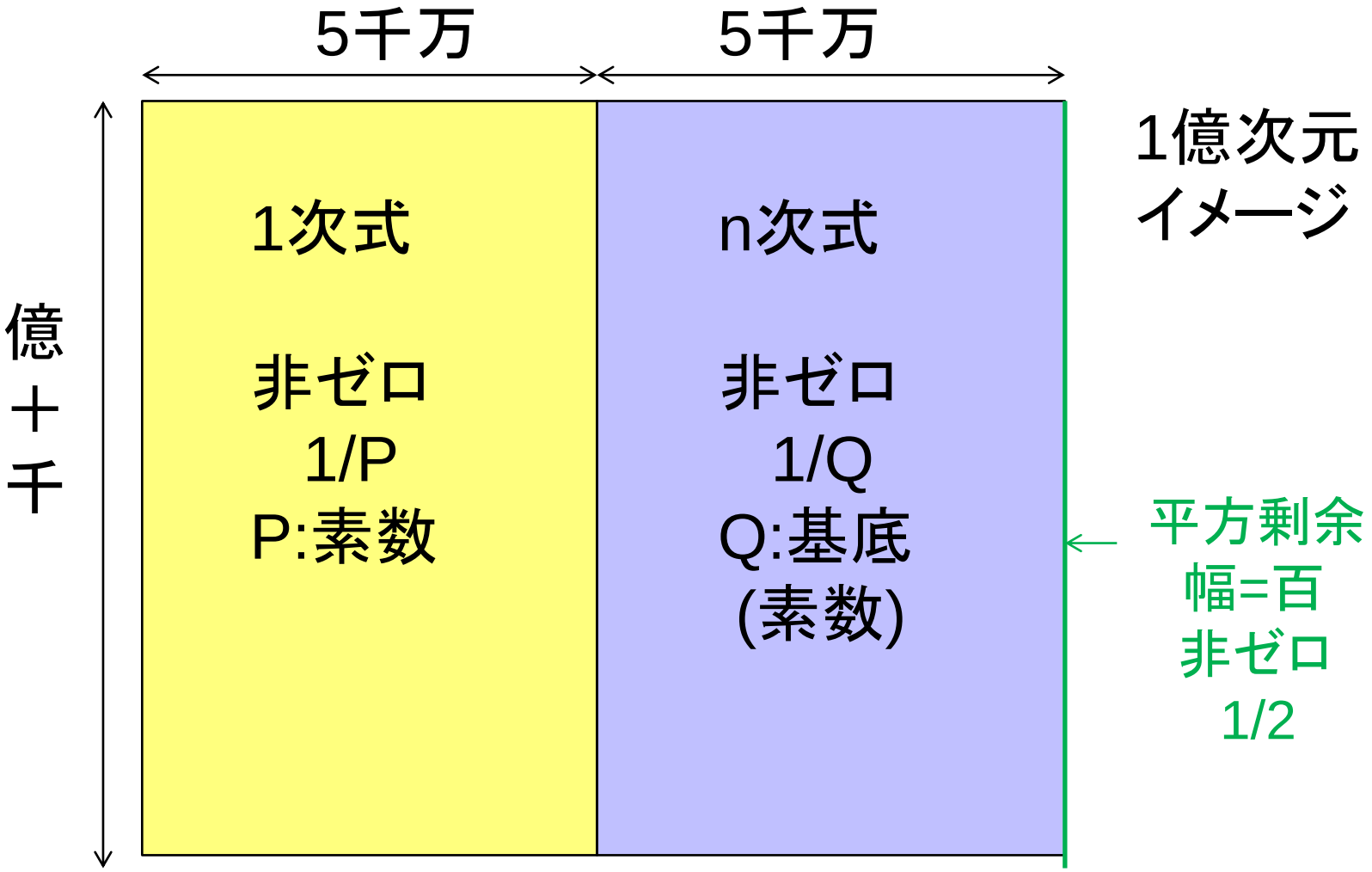
  $|a^n f(-b/a)|$とbA-aBを基底で分解 →現方式

3. 1次式＋n次式のGNFS

- AM+B=N,n次式f(M)=0 (mod N)のMと係数探査
- ふるい処理 (基底でaB-bA, $|a^n f(-b/a)|$を基底分解)
  gcd(a,b)=1で動かす。基底はP以下の素数とその部分集合
- 0-1行列の線形方程式から複数の解を求める
- $t(x)^2=d(x) \pmod{f(x)}$の解t(x)。d(x)は線形解より
- $S^2 - T^2 = 0 \pmod{N}$よりNを因数分解

注) Nは分解対象数。F(x)は現在6次式を使用
因数分解できる確率は50% → 複数解が必要

3. GNFSの行列の形（1次式）



3. RSA-768の計算規模(1次式)

項目	台数･年	比(%)
ふるい処理	1500	90
0-1行列の線形計算	155	9
利用関数の探査	20	1
代数平方根の計算	1	0
その他	1	0

注) AMD64 (2.2Ghz, 1コア換算)
行列サイズ：192,796,550×192,795,550

3. 0-1行列の線形計算(1次式)

- 目的

  基底のベキを偶数 → $S^2 = T^2 \pmod N$
- 計算方法

  (a) 反復解法(◎)　　(b) 直接解法(×)
- サイズ

  (a) RSA-768(232桁)　→ 2億次元

  (b) RSA-1024(309桁) → 100億次元

4. 2次式+n次式のGNFS

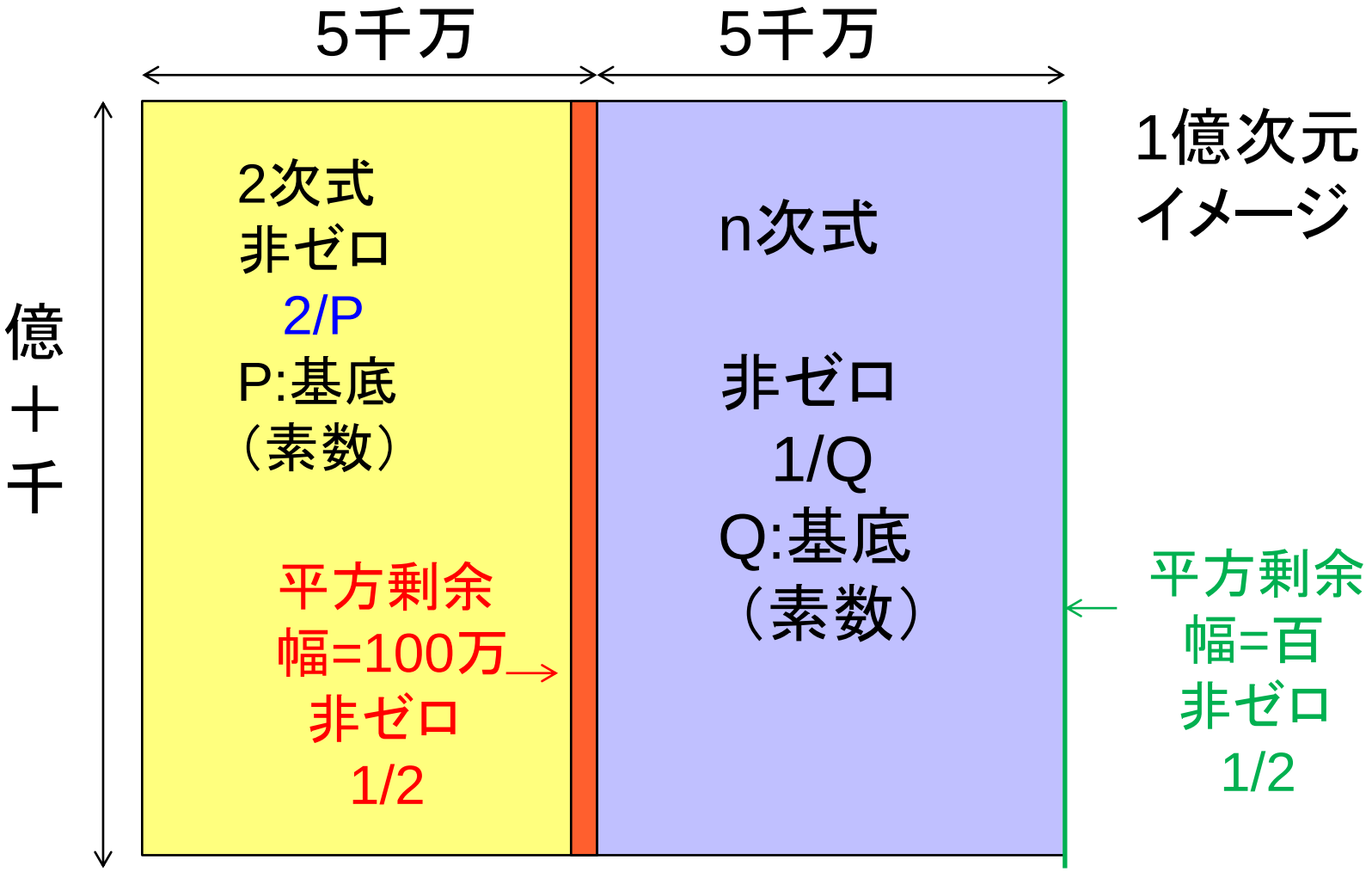
- 2次式g(M)=0,n次式f(M)=0 (mod N)のMと係数探査
- ふるい処理 (基底で$|a^2g(-b/a)|$, $|a^nf(-b/a)|$を分解)

  gcd(a,b)=1で動かす。基底はP以下の素数の部分集合
- 0-1行列の線形方程式から複数の解を求める
- $t(x)^2=d(x)$ (mod f(x))の解t(x)。d(x)は線形解より

  $s(x)^2=e(x)$ (mod g(x))の解s(x)。e(x)は線形解より
- $S^2 - T^2 = 0$ (mod N)よりNを因数分解

注) Nは分解対象数。1次+n次より小さい係数が可能

4. GNFSの行列の形（2次式）



4. 0-1行列の線形計算(2次式)

- 目的

  基底のベキを偶数 → $S^2 = T^2 \pmod N$
- 計算方法

  (a) 反復解法(×)　　(b) 直接解法(〇)
- 直接解法が有利になる理由

  ふるい結果の平方剰余(0,1が半々)を追加 →

  2次式は多数(数百万?)、3次式以上は数十 →

  非ゼロ要素数の増加 → 直接解法が有利

5. 多項式の係数の大きさ

- m次とn次の多項式の組合せ
- g(M) = 0 (mod N), f(M) = 0 (mod N)

  $g(x) = A_0x^m + A_1x^{m-1} + \ldots + A_{m-1}x + A_m$

  $f(x) = B_0x^n + B_1x^{n-1} + \ldots + B_{n-1}x + B_n$
- $\max(|A_i|, |B_j|) = C, \quad i=0,..,m,\ j=0,\ldots,n$
- Cを小さくできる限界

  $C = O(N^{1/(n+m)})$ ： Nの(n+m)乗根

5. 1次+n次多項式の係数

- 1次式とn次式

  $g(M) = A_0M + A_1 = 0 \pmod N$

  $f(M) = B_0M^n + B_1M^{n-1} + \ldots + B_{n-1}M + B_n = 0 \pmod N$

- $A_0M+A_1=0$ → $M=-A_1/A_0 \pmod N$を$f(M)$に代入

  $|A_0^n f(M)| = |A_1^n B_0 - A_1^{n-1}A_0B_1 + \ldots + A_0^nB_n| = \alpha N$

- 係数A_i,B_jの最小化の限界($\alpha=1$が最小)

  $\max(|A_i|)=A, \max(|B_j|=B$ → $c_1=(A^nB)^{1/(n+1)} > (N/(n+1))^{1/(n+1)}$

- A=Bのときの限界

  $A, B > (N/(n+1))^{1/(n+1)}$

5. 2次+n次多項式の係数

- 2次式とn次式

  $g(M) = A_0M^2 + A_1M + A_2 = 0 \pmod N$

  $f(M) = B_0M^n + B_1M^{n-1} + \ldots + B_{n-1}M + B_n = 0 \pmod N$

- 1次式の類推で精密な下限を推定 → 例で裏付け
- 係数A_i,B_jの最小化の限界

  $\max(|A_i|)=A, \max(|B_j|=B \rightarrow c_2=(A^nB^2)^{1/(n+1)} > (N/(n+1))^{1/(n+1)}$

- A=Bのときの限界

  $A, B > (N/(n+1))^{1/(n+2)}$ ← $(N/(n+1))^{1/(n+1)}$:1次式

6. 係数の例（15桁、4次式）

- N=447482215496831
- 4次式(n=4),　　下限=617,　$n^{1/5}$=851 ,　$n^{1/6}$=277
- 1次式+4次式 (M=154435163481227, xで表示)

  $707x - 725 = 0$　　c_1=688

  $85x^4 + 556x^3 + 556x^2 + 31x + 481 = 0 \pmod N$
- 2次式+4次式 (M=439202295239286, xで表示)

  $120x^2 - 193x + 193 = 0$　　c_1=198, c_2=689

  $257x^4 + 334x^3 + 290x^2 + 15x - 73 = 0 \pmod N$

6. 係数の例（15桁、5次式）

- N=447482215496831　　以下(mod N)は省略
- 5次式(n=5),　　下限=205, $n^{1/6}$=277 , $n^{1/7}$=124
- 1次式+5次式 (M=326598394248873, xで表示)

  $211x - 229 = 0$　　c_1=226

  $110x^5 + 108x^4 + 124x^3 + 175x^2 + 162x + 214 = 0$
- 2次式+5次式 (M=215647630140378, xで表示)

  $66x^2 - 7x + 76 = 0$　　c_1=87, c_2=207

  $163X^5 - 26x^4 - 125x^3 + 176x^2 + 136x - 85 = 0$

6. 係数の例（20桁、5次式）

- N=29352161663088766301
- 5次式(n=5),　　下限=1303,　$n^{1/6}$=1756 ,　$n^{1/7}$=604
- 1次式+5次式 (M=245980877567027332 93, xで表示)

  1383x – 1360 = 0　　c_1=1381

  $1307x^5 + 411x^4 + 1078x^3 + 1047x^2 + 148x + 1370 = 0$
- 2次式+5次式 (M=139010811250747390 00, xで表示)

  $546x^2 – 775x + 690 = 0$　　c_1=655, c_2=1678

  $167X^5 – 168x^4 – 7x^3 + 283x^2 – 266x – 61 = 0$

7. GNFS(1次式+n次式)の特徴

- 利点（2次式+n次式と比較）

  AM+B=0からM=-B/A (mod N)で計算容易

  追加平方剰余は1次式が0で、n次式も小 →

  非ゼロ要素数が小 → 0-1行列反復解法

- 欠点（2次式+n次式と比較）

  最小係数限界がO($N^{1/(n+1)}$)と大きい →

  → ふるい処理が大（0-1行列の次元数大)

7. GNFS(2次式+n次式)の特徴

- 利点（1次式+n次式と比較）

  最小係数限界がO($N^{1/(n+2)}$)と小さい →

  → ふるい処理が小（0-1行列の次元数小)

  (値(1次式=bA-aB,2次式=|b^2A-abB+a^2B|)大だが、ふるい間隔が半分とfree relation多数で、1次式とふるい効率は同程度)

- 欠点（1次式+n次式と比較）

  Mと2次式の計算が困難（探索手法が未知）

  2次式は平方剰余の追加が多数 →

  非ゼロ要素数が大 → 0-1行列直接解法

8. おわりに

- 1次式及び2次式+n次式のGNFSの係数

  1次式使用 → 1次式、n次式係数 = $O(N^{1/(n+1)})$

  2次式使用 → 2次式、n次式係数 = $O(N^{1/(n+2)})$

- 2次式+n次式の係数探査の見込み

  (1) 最良方法 → 見込みなし

  2次式係数=$O(N^{1/(n+2)})$，n次式係数=$O(N^{1/(n+2)})$

  (2) 次善方式 → 今回見込みがつく

  2次式係数=$O(N^{1/(n+3)})$，n次式係数=$O(N^{1/(n+1)})$