2次ふるい法による因数分解

2008年8月6日

東京工芸大学
後 保範

1. QSとMPQS

(1) 分解対象数をNとする

(2) QS(2次ふるい法)

$M=N^{1/2}$, $(M+k)^2 - N = S_k$, $k=1,2,\ldots,L$

S_kを素数基底で分解

(3) MPQS(複数多項式2次ふるい法)

$f_h(x) = \{(ax+b_h)^2 - N\}/a$, $x=-L,..,-1,0,1,..,L$

$f_h(x)$を素数基底で分解

$b_k^2 - N \equiv 0 \pmod{a_k}$より$a,b_h$を作成

2. QSによる因数分解例

(1) 分解対象数(N)

$N = 480923, \quad M = [\, N^{1/2} \,] = 694$

(2) 素数基底

Pが53以下の素数で、b<Pの整数bが

$b^2 - N \equiv 0 \pmod{P}$を満たすPを使用

素数基底は下記の10個となる

{ 2, 7, 11, 13, 23, 29, 31, 37, 43, 53}

3. QSによるふるい結果

No	x	x^2-N	2	7	11	13	23	29	31	37	43	53
0	694	713	0	0	0	0	1	0	1	0	0	0
1	701	10478	1	0	0	2	0	0	1	0	0	0
2	709	21758	1	0	1	0	1	0	0	0	1	0
3	710	23177	0	2	1	0	0	0	0	0	1	0
4	732	54901	0	1	1	0	1	0	1	0	0	0
5	753	86086	1	1	1	1	0	0	0	0	1	0
6	787	138446	1	1	1	0	0	1	1	0	0	0
7	794	149513	0	1	0	1	0	0	1	0	0	1
8	808	171941	0	2	2	0	0	1	0	0	0	0
9	809	173558	1	3	1	0	1	0	0	0	0	0
10	924	372853	0	0	0	1	1	1	0	0	1	0

3.1 ふるいの説明

(1) $x = 694 = M$

$x^2 - N = 694^2 - 480923 = 713 = 23 \cdot 31$

(2) $x = 701 = M+7$

$x^2 - N = 701^2 - 480923 = 10478$

$= 2 \cdot 13^2 \cdot 31$

(3) $x = 709 = M+15$

$x^2 - N = 709^2 - 480923 = 21758$

$= 2 \cdot 11 \cdot 23 \cdot 43$

4. 行列計算

- ふるい結果の2の剰余行列(A)

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

4.1 行列消去

(1) ふるい結果の2の剰余行列(A+E)
  (a) ふるい結果に対し(mod 2)の行列 → A
  (b) 行列Aの右に対角行列(E)を追加
(2) 行列消去
  (a) A+Eの行列をガウス消去法で消去
  (b) 軸交換し、対角行は必ず1にする
      → 総てゼロなら消去完了
  (c) (軸+1)の行と列以下を軸列で消去
  (d) 消去完なら行列Eに従属情報が入る

4.2 消去結果

- ふるい結果の2の剰余行列(A+E)

A	E
1 0 0 0 0 0 1 0 0 0	0 1 0 0 0 0 0 0 0 0 0
0 1 1 0 1 0 1 0 0 0	0 0 0 0 1 0 0 0 0 0 0
0 0 1 0 1 0 1 0 1 0	0 1 1 0 0 0 0 0 0 0 0
0 0 0 1 1 0 0 0 1 0	0 1 0 0 1 1 0 0 0 0 0
0 0 0 0 1 0 1 0 0 0	1 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 1 0 0 0 0	1 1 0 0 1 0 1 0 0 0 0
0 0 0 0 0 0 0 0 0 1	1 0 1 0 0 1 0 1 0 0 0
0 0 0 0 0 0 0 0 0 0	1 1 1 1 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0	1 1 0 0 1 0 1 0 1 0 0
0 0 0 0 0 0 0 0 0 0	0 1 0 0 1 0 0 0 0 1 0
0 0 0 0 0 0 0 0 0 0	1 0 0 0 0 1 1 0 0 0 1

4.4 従属行の取り出し

(1) 消去結果(Aが総てゼロ)　　E

7	0 0 0 0 0 0 0 0 0 0 0	1 1 1 1 0 0 0 0 0 0
8	0 0 0 0 0 0 0 0 0 0 0	1 1 0 0 1 0 1 0 1 0 0
9	0 0 0 0 0 0 0 0 0 0 0	0 1 0 0 1 0 0 0 0 1 0
10	0 0 0 0 0 0 0 0 0 0 0	1 0 0 0 0 1 1 0 0 0 1

(2) 従属行の取り出し(Eの1の行を取り出し)

(a) 7行:　0, 1, 2, 3

(b) 8行:　0, 1, 4, 6, 8

(c) 9行:　1, 4, 9

(d) 10行:　0, 5, 6, 10

5. 因数分解

(1) 従属行を使用し下記のX,Yの値を計算

$X^2 - Y^2 \equiv 0 \pmod N$

(a) Xの計算(従属行から単純計算)

ふるい結果の左辺(x)の乗算

(b) Yの計算(従属行の素数基底のベキ計算)

各基底ベキ数=(従属行の各基底ベキの合計)/2

(2) P=GCD(X+Y, N), Q=GCD(X-Y,N)

→ P×Q=Nと因数分解

ただし、半分は自明解となる

5.1 因数分解例1

- 従属行(0,1,2,3行)での因数分解

(1) Xの計算(従属行から単純計算)

X = 694･701･709･710 (mod N) = 123677

(2) Yの計算(従属行の素数基底のベキ計算)

基底 = 2, 7, 11, 13, 23, 29, 31, 37, 43, 53

ベキ = (2, 2, 2, 2, 2, 0, 2, 0, 2, 0) / 2

Y = 2･7･11･13･23･31･43 (mod N) = 302097

(3) P = GCD(X+Y,N)

P = GCD(123677+302097, 480923) = 593

→ P=593, Q=811 とNは因数分解

5.2 因数分解例2

- 従属行(0,1,4,6,8行)での因数分解

(1) Xの計算(従属行から単純計算)

$X = 694 \cdot 701 \cdot 732 \cdot 787 \cdot 809 \pmod N = 411532$

(2) Yの計算(従属行の素数基底のベキ計算)

基底 = 2, 7, 11, 13, 23, 29, 31, 37, 43, 53

ベキ = (2, 4, 4, 2, 2, 2, 4, 0, 0, 0) / 2

$Y = 2 \cdot 7^2 \cdot 11^2 \cdot 13 \cdot 23 \cdot 29 \cdot 31^2 \pmod N = 270418$

(3) P = GCD(X+Y,N)

P = GCD(411532+270418, 480923) = 593

→ P=593, Q=811 とNは因数分解

5.3 因数分解結果

(1) 従属行(0,1,2,3行)

X=123677, Y=302097, N=593・811と因数分解

(2) 従属行(0,1,4,6,8行)

X=411532, Y=270418, N=593・811と因数分解

(3) 従属行(1,4,9行)

X=87239, Y=373522, N=593・811と因数分解

(4) 従属行(0,5,6,10行)

X=104199, Y=104199, 自明解で分解できず