多数桁数因数分解における 0-1行列の疎行列直接解法

2006年6月15日

渡邊 裕介(早稲田大学)
後　保範 (早稲田大学)

目 次

1. はじめに

1. RSA暗号の解読
   → 多数桁数の因数分解
   → GNFS,MBPS等の篩法
2. 篩法
   (1) 篩で必要データを集める
   (2) 0-1係数の行列から従属行を求める
   (3) $x^2 \equiv y^2 \pmod N$を作成し、Nを因数分解

1.1 0-1行列の従属行の計算

1. 現在使用されている方式(PCクラスタが前提)
   ブロック･ランチョス法
   200桁の因数分解
   → 64M次元(平均非ゼロ数: 172/行)
2. 発表する方法(スーパーコンの使用を前提)
   疎行列直接解法(ガウス消去法)
   目標: 200M次元/4TB
   平均非ゼロ数: 180/行
   使用メモリ量: 4TB(500倍まで密化可能)
   64ビット整数に64データ (5データ/バイト)
   (配列ポインタは32ビット整数)

2. 従属行の算出と因数分解

- 多数桁数因数分解の手順

1. MBPS,GNFS等で必要データを集める
   MBPS: Multiple Base Polynomial Sieve
   GNFS: General Number Field Sieve
2. 法2の行列Aを作成する
3. 行列Aを消去する
4. 消去結果から従属行を取り出す
5. 従属行を使用し因数分解する

2.1 篩法で必要データ収集

- N=1333を因数分解する例

1. $f(x)=3x^2+10$, $f(M)=1333$, $M=21$を使用
2. $(3M+a)(M+b)\equiv sM+t \pmod M$で篩を実施

   $s=a+3b$, $t=ab-10$
3. 素数基底は-1,2,3,5,7,11,13の6個

   1次基底は$3M-10=53$の1個
4. $(3M-10)(M+5) \equiv 5M-60 \rightarrow 2\cdot 13(3M-10)=3^2\cdot 5$

   $(3M-10)(M+6) \equiv 6M-70 \rightarrow 3^3(3M-10)=2\cdot 7^2$

- - - - -

2.2 篩の結果

No.	係数		素数基底及び一次式基底							
	a	b	−1	2	3	5	7	11	13	53
1	−10	5	0	1	−2	−1	0	0	1	1
2	−10	6	0	−1	3	0	−2	0	0	1
3	0	0	1	−1	3	−1	2	0	0	0
4	1	0	0	6	1	0	1	−1	0	0
5	1	1	0	7	−1	−2	0	1	0	0
6	2	0	0	−5	1	1	1	0	1	0
7	3	−1	1	3	1	1	0	1	−1	0
8	0	1	0	1	2	0	1	1	0	−1

例: $2 \cdot 13 \cdot 53 = 3^2 \cdot 5 \pmod{1333}$

2.3 (mod 2)行列A+I

行番号	A	+	I
1	0 1 0 1 0 0 1 1		1 0 0 0 0 0 0 0
2	0 1 1 0 0 0 0 1		0 1 0 0 0 0 0 0
3	1 1 1 1 0 0 0 0		0 0 1 0 0 0 0 0
4	0 0 1 0 1 1 0 0		0 0 0 1 0 0 0 0
5	0 1 1 0 0 1 0 0		0 0 0 0 1 0 0 0
6	0 1 1 1 1 0 1 0		0 0 0 0 0 1 0 0
7	1 1 1 1 0 1 1 0		0 0 0 0 0 0 1 0
8	0 1 0 0 1 1 0 1		0 0 0 0 0 0 0 1

2.4 行列の消去結果

行番号	A	+	I
1	1 1 1 1 0 0 0 0		0 0 1 0 0 0 0 0
2	0 1 1 0 0 0 0 1		0 1 0 0 0 0 0 0
3	0 0 1 1 0 0 1 0		1 1 0 0 0 0 0 0
4	0 0 0 1 1 1 1 0		1 1 0 1 0 0 0 0
5	0 0 0 0 0 1 0 1		0 1 0 0 1 0 0 0
6	0 0 0 0 0 0 1 1		0 1 1 0 1 0 1 0
7	0 0 0 0 0 0 0 0		1 1 0 1 1 1 0 0
8	0 0 0 0 0 0 0 0		0 1 0 1 0 0 0 1

2.5 従属行の取り出し

1. 7行目より

   1 1 0 1 1 1 0 0 (消去後のIの7行目)

   → 従属行は1,2,4,5,6行 (1の対応行)

2. 8行目より

   0 1 0 1 0 0 0 1 (消去後のIの7行目)

   → 従属行は2,4,8行 (1の対応行)

2.6 因数分解

1. 1,2,4,5,6行から

   $(2^4 \cdot 3 \cdot 13 \cdot 53)^2 \equiv 5^2 \pmod{1333}$

   → $253^2 \equiv 5^2 \pmod{1333}$

   → $1333 \equiv 31 \cdot 43$: $253 - 5 = 8 \cdot 31$

2. 2,4,8行から

   $(2^3 \cdot 3^3)^2 \equiv 1^2 \pmod{1333}$

   → $216^2 \equiv 1^2 \pmod{1333}$

   → $1333 \equiv 31 \cdot 43$: $216 - 1 = 5 \cdot 43$

3. ガウス消去法の工夫

1. 行列n×m次元行列Aで消去する
2. 長さnとmのベクトルを用意する
3. 軸交換と枢軸情報をベクトルに保持
4. 枢軸をksとし消去は下記

$$A_{ij} = A_{ij} - A_{is} \cdot A_{kj} \pmod 2, \quad i>k, \ j \neq s$$

5. 消去完了行以下に従属行の情報
6. 両ベクトルで本来の従属行情報に変換

3.1 消去前の行列

交換	行列A							
1	0	1	0	1	0	0	1	1
2	0	1	1	0	0	0	0	1
3	1	1	1	1	0	0	0	0
4	0	0	1	0	1	1	0	0
5	0	1	1	0	0	1	0	0
6	0	1	1	1	1	0	1	0
7	1	1	1	1	0	1	1	0
8	0	1	0	0	1	1	0	1

枢軸 ←								
	0	0	0	0	0	0	0	0

3.2 消去過程(1/5)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	0	1	0	0	1	1
4	0	0	1	0	1	1	0	0
5	0	1	1	0	0	1	0	0
6	0	1	1	1	1	0	1	0
7	1	0	0	0	0	1	1	0
8	0	1	0	0	1	1	0	1

枢軸 ―								
	3	0	0	0	0	0	0	0

3.3 消去過程(2/5)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	0
4	0	0	1	0	1	1	0	0
5	0	1	0	0	0	1	0	1
6	0	1	0	1	1	0	1	1
7	1	0	0	0	0	1	1	0
8	0	1	1	0	1	1	0	0

枢軸 ←	3	2	0	0	0	0	0	0

3.4 消去過程(3/5)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	0
4	0	1	1	1	1	1	1	0
5	0	1	0	0	0	1	0	1
6	0	1	0	1	1	0	1	1
7	1	0	0	0	0	1	1	0
8	0	0	1	1	1	1	1	0

枢軸								
←	3	2	1	0	0	0	0	0

3.5 消去過程(4/5)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	0
4	0	1	1	1	1	1	1	0
5	0	1	0	0	0	1	0	1
6	0	0	1	1	0	1	0	1
7	1	0	0	0	0	1	1	0
8	0	1	0	1	0	0	0	0

枢軸 ←								
	3	2	1	4	0	0	0	0

3.6 消去過程(5/5)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	0
4	0	1	1	1	1	1	1	0
5	0	1	0	0	0	1	0	1
6	0	1	1	1	0	1	0	0
7	1	1	0	0	0	1	1	1
8	0	1	0	1	0	0	0	0
枢軸	3	2	1	4	0	5	0	0

3.7 消去結果

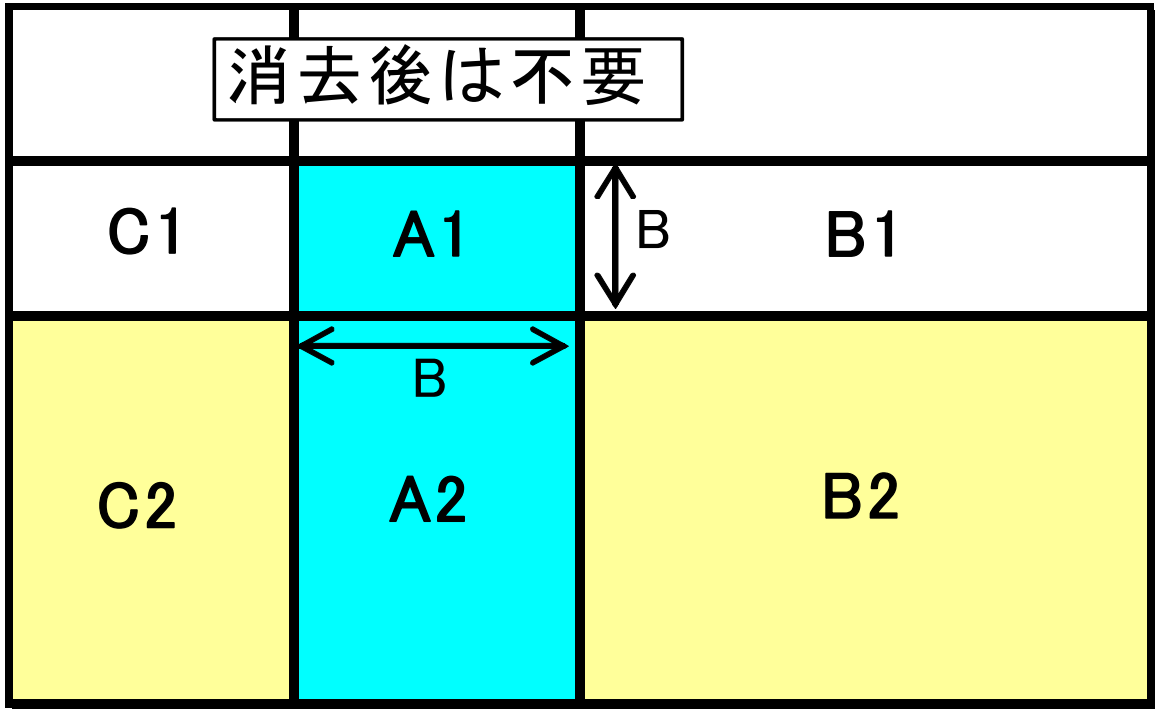
交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	0
4	0	1	1	1	1	1	1	0
5	0	1	0	0	0	1	0	1
7	1	1	0	0	0	1	1	1
6	0	1	1	1	0	1	0	0
8	0	1	0	1	0	0	0	0

枢軸	3	2	1	4	0	5	7	0

従属行1: 1, 2, 4, 5, 6

従属行2: 2, 4, 8

4. ブロック・ガウス消去法



1. A1,A2の消去
2. B2=B2−A2・B1 (mod 2)で消去
3. C2=C2−A2・B1 (mod 2)で消去

4.1 消去前の行列

交換	行列A							
1	0	1	0	1	0	0	1	1
2	0	1	1	0	0	0	0	1
3	1	1	1	1	0	0	0	0
4	0	0	1	0	1	1	0	0
5	0	1	1	0	0	1	0	0
6	0	1	1	1	1	0	1	0
7	1	1	1	1	0	1	1	0
8	0	1	0	0	1	1	0	1

枢軸								
←	0	0	0	0	0	0	0	0

4.2 ブロック消去過程(1/4)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	1
4	0	1	1	0	1	1	0	0
5	0	1	0	0	0	1	0	0
6	0	1	0	1	1	0	1	0
7	1	0	0	1	0	1	1	0
8	0	0	1	0	1	1	0	1

枢軸								
	3	2	1	0	0	0	0	0

4.3 ブロック消去過程(2/4)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	1
4	0	1	1	1	1	1	1	0
5	0	1	0	0	0	1	0	1
6	0	1	0	1	1	0	1	1
7	1	0	0	0	0	1	1	0
8	0	0	1	1	1	1	1	0

枢軸								
←	3	2	1	0	0	0	0	0

4.4 ブロック消去過程(3/4)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	1
4	0	1	1	1	1	1	1	0
5	0	1	0	0	0	1	0	1
6	0	1	0	1	0	1	1	1
7	1	0	0	0	0	1	1	0
8	0	0	1	1	0	0	1	0
枢軸	3	2	1	4	0	5	0	0

4.5 ブロック消去過程(4/4)

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	1
4	0	1	1	1	1	1	1	0
5	0	1	0	0	0	1	0	1
6	0	1	1	1	0	1	0	0
7	1	1	0	0	0	1	1	1
8	0	1	0	1	0	0	0	0

枢軸								
←	3	2	1	4	0	5	0	0

4.6 ブロック消去結果

交換	行列A							
3	1	1	1	1	0	0	0	0
2	0	1	1	0	0	0	0	1
1	0	1	1	1	0	0	1	1
4	0	1	1	1	1	1	1	0
5	0	1	0	0	0	1	0	1
7	1	1	0	0	0	1	1	1
6	0	1	1	1	0	1	0	0
8	0	1	0	1	0	0	0	0

枢軸	3	2	1	4	0	5	7	0

従属行1: 1, 2, 4, 5, 6

従属行2: 2, 4, 8

5. 疎行列ガウス消去法

- 現在検討中
- 配列の持ち方(疎行列のデータ圧縮)
  → 2次元配列(消去更新の効率化)
  → 自然な溢れ対策
  → 64ビット整数に64個詰め
  (ポインターは32ビット整数)
- 排他和演算で64データの一括処理
- 非ゼロ要素を削減する番号付け検討中

6. おわりに

- 因数分解で発生する0-1行列計算
- 疎行列の直接解法を使用
- ブロック化ガウス消去法
- 64ビット整数に64データ詰め
  ポインタは32ビット整数
- 排他和命令で64データを一括処理
- 疎行列形式と番号付けは検討中