SIQS(自己初期化 2 次篩法)による因数分解例

2006/3/24 後 保範(早稲田大学)

1. 概要

合成数 N に対して 2 次関数 $f(x)$ を使用して篩を行い、因数分解する。

$$b_j^2 - N = 0 \mod p_j,\ j = 1,2,\cdots,M$$

となる整数 b_j が存在(平方剰余)する p_j を小さい方の素数から求める。

p_j の中の数個を乗算したものを A とし、b は $b^2 - N = 0 \mod A$ から求める。

このとき、A,b は多数作成することができる。各 A,b に対して下記が成立する。

$$F(x) = (Ax+b)^2 - N = A \cdot f(x)$$
$$f(x) = Ax^2 + Bx + C,\quad B = 2b,\ C = F(0)/A$$

$$(Ax+b)^2 = A \cdot f(x) \mod N$$

各 A,b により得られる $f(x)$ を-1 と素数基底($p_j, j = 1,2\cdots,M$)で分解し基底の数(M+1)より多く集める。その後、$A \cdot f(x)$ の素数基底のベキが偶数になるよう、0-1 行列の従属行を求め、$s^2 = t^2 \mod N$ の形にして因数分解する。s^2 は $(Ax+b)^2$ から求め、t^2 は $A \cdot f(x)$ から求める。

ここでは、説明を単純にするため 2 次多項式 $f(x)$ は 1 個だけの例を示す。

2. 計算対象と分解関数

$N = 55751$ を SIQS で因数分解する。

p を 71 以下の素数とし、N の平方剰余($b^2 - N = 0 \mod p$ となる b が存在する)となるものを求め、-1 と合わせて素数基底にする。

素数基底 = (-1, 2, 5, 11, 17, 19, 29, 41, 43, 47, 61, 71)

ここでは、A は 1 個の素数で作成し単一の関数 $f(x)$ を使用する。

$A = 11$ とすると $5^2 - N = 0 \mod 11$ となり下記が得られる。

$$(11x+5)^2 = 11 \cdot f(x) \mod N$$
$$f(x) = 11x^2 + 10x - 5066,\ C = (5^2 - N)//11 = -5066$$

3．SIQS による篩

(1) $f(b)=0 \mod p$ の計算

一般には複数多項式を使用し、$f(b)=0 \mod p$ となる b は $b^2-N=0 \mod p$ から変換して求めるが、ここでは 1 個の多項式なので $f(b)=0 \mod p$ から直接求める。b が小さい範囲では $b=0,1,2,\cdots,p-1$ としてテストし、大きくなると法 p の平方根を計算することで求める。$f(b)=0 \mod p$ となる b を表 1 に示す。このとき、p のベキ乗に対しても b が小さければ求めておく。

表 1.　$f(b)=0 \mod p$ となる b の値

p	2	5	5^2	5^3	11	11^2	17	19	29	29^2	41	41^2	43	47	61	71
b	0	1	4	11	5	-17	0	-3	-4	-18	2	12	-6	-5	2	-13
	--	-1	11	--	--	--	-4	9	11	--	12	--	9	-13	-14	25

(2) $f(x)$ の素数基底による篩

x を-30 から 30 まで動かし $f(x)$ を素数基底で分解するための篩を行う。

$f(x)$ が表 1 の p で割れる条件は、整数 α に対して $x=\alpha p+b$ が成立すればよい。

そのため、b を基点にして p 飛びに篩(ふるい)を実施する。

篩の詳細は SIQS による篩例を参照。

4．従属行の決定

(1) 分解関係行列

$(11x+5)^2=11\cdot f(x)$ に $f(x)$ の篩結果をあてはめると表 2 の行列が得られる。

表 2．分解関係行列

No.	x	f(x)	素数基底												平方数
			-1	2	5	11	17	19	29	41	43	47	61	71	|11x+5|
1	-29	3895	0	0	1	1	0	1	0	1	0	0	0	0	314
2	-22	38	0	1	0	1	0	1	0	0	0	0	0	0	237
3	-21	-425	1	0	2	1	1	0	0	0	0	0	0	0	226
4	-18	-1682	1	1	0	1	0	0	2	0	0	0	0	0	193
5	-17	-2057	1	0	0	3	1	0	0	0	0	0	0	0	182
6	-14	-3050	1	1	2	1	0	0	0	0	0	0	1	0	149
7	-13	-3337	1	0	0	1	0	0	0	0	0	1	0	1	138
8	-6	-4730	1	1	1	2	0	0	0	0	1	0	0	0	61
9	-4	-4930	1	1	1	1	1	0	1	0	0	0	0	0	39
10	2	-5002	1	1	0	1	0	0	0	1	0	0	1	0	27
11	9	-4085	1	0	1	1	0	1	0	0	1	0	0	0	104
12	11	-3625	1	0	3	1	0	0	1	0	0	0	0	0	126
13	12	-3362	1	1	0	1	0	0	0	2	0	0	0	0	137
14	16	-2090	1	1	1	2	0	1	0	0	0	0	0	0	181
15	21	-5	1	0	1	1	0	0	0	0	0	0	0	0	236
16	25	2059	0	0	0	1	0	0	1	0	0	0	0	1	280

(2) 従属行計算行列

表 2 の素数基底に対応する部分の 2 の剰余から下記の行列が作成される。

```
        0 0 1 1 0 1 0 1 0 0 0 0
        0 1 0 1 0 1 0 0 0 0 0 0
        1 0 0 1 1 0 0 0 0 0 0 0
        1 1 0 1 0 0 0 0 0 0 0 0
        1 0 0 1 1 0 0 0 0 0 0 0
        1 1 0 1 0 0 0 0 0 0 1 0
        1 0 0 1 0 0 0 0 0 1 0 1
  A  =  1 1 1 0 0 0 0 0 1 0 0 0
        1 1 1 1 1 0 1 0 0 0 0 0
        1 1 0 1 0 0 0 1 0 0 1 0
        1 0 1 1 0 1 0 0 1 0 0 0
        1 0 1 1 0 0 1 0 0 0 0 0
        1 1 0 1 0 0 0 0 0 0 0 0
        1 1 1 0 0 1 0 0 0 0 0 0
        1 0 1 1 0 0 0 0 0 0 0 0
        0 0 0 1 0 0 1 0 0 0 0 1
```

(3) 行列消去

単位行列をＥとする、行列Ａの右にＥを追加して行列ＡをＥと合わせて消去する。

行列ＡとＥの消去結果を下記に示す。

```
                A                                E
1 0 0 1 1 0 0 0 0 0 0 0   0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
0 1 0 1 0 1 0 0 0 0 0 0   0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 1 1 0 1 0 1 0 0 0 0   1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 1 1 1 0 0 0 0 0 0   0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 1 0 0 0 0 1 0 1   0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0
0 0 0 0 0 1 0 1 1 0 0 0   1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0
0 0 0 0 0 0 1 1 0 0 0 0   1 1 1 0 0 0 0 0 1 0 0 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 1 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 1 1 0 0   0 0 1 0 0 0 1 1 1 0 0 0 0 0 0 1
0 0 0 0 0 0 0 0 0 0 0 1 0   0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0
      Eの列番号 -->         1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
0 0 0 0 0 0 0 0 0 0 0 0 0   0 1 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 0 1 1 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 0 1 0 0 0 0 0 0 0 0 1 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0   1 0 0 1 0 1 0 0 0 1 0 0 0 1 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0   1 1 0 1 0 1 0 0 0 1 0 0 0 0 1 0
0 0 0 0 0 0 0 0 0 0 0 0 0   0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0
```

(4) 従属行

行列消去し、行列Ａが全てゼロになった行のＥの行で非ゼロとなる列が従属行を示す。従って、従属行は 6 組あり次のようになる。

従属行１： 2, 8, 11

従属行２： 3, 4, 9, 12

従属行３： 4, 13

従属行４： 1, 4, 6, 10, 14

従属行５： 1, 2, 4, 6, 10, 15

従属行６： 3, 5

5. 因数分解

(1) 従属行１：2,8,11

表 2 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(237*61*104)^2 = (2*5*11^2*19*41)^2$

$54202^2 = 40803^2 \mod 55751$

従って N は下記のように因数分解できる。

GCD(54202+40803,55751) = 283

GCD(54202-40803,55751) = 197

(2) 従属行２： 3,4,9,12

表 2 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(226*193*39*126)^2 = (2*5^3*11^2*17*29)^2$

$32008^2 = 23743^2 \mod 55751$

32008+23743=55751 で自明の関係となり因数分解できない。

(3) 従属行３：4,13

表 2 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(193*137)^2 = (2*11*29*41)^2$

$26441^2 = 26158^2 \mod 55751$

従って N は下記のように因数分解できる。

GCD(26441+26158,55751) = 197

GCD(26441-26158,55751) = 283

(4) 従属行４：1,4,6,10,14

表 2 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(314*193*149*27*181)^2 = (2^2*5^2*11^3*19*29*41*61)^2$

$46855^2 = 28140^2 \mod 55751$

従って N は下記のように因数分解できる。

GCD(46855+28140,55751) = 283

GCD(46855-28140,55751) = 197

(5) 従属行５：1,2,4,6,10,15

表 2 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(314*237*193*149*27*236)^2 = (2^2*5^2*11^3*19*29*41*61)^2$

$46855^2 = 28140^2 \mod 55751$

この結果は(4)と同一。

(6) 従属行６：3,5

表 2 に従属行を当てはめ、N=55751 を法とすると下記の関係が成立する。

$(226*182)^2 = (5*11^2*17)^2$

$41132^2 = 10285^2 \mod 55751$

従って N は下記のように因数分解できる。

GCD(41132+10285,55751) = 197

GCD(41132-10285,55751) = 283