SIQS(自己初期化 2 次篩法)による篩例 1

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)する素数 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)

素数 3,7,13,23,31,37,53,59,67 は N が非平方剰余なので素数基底に入れない。

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。篩は表 2 に示す各素数基底のテーブルを 1 にしておき、その素数で割れる(p 飛びの篩)と素数の値を 1 の代わりにセットする。素数のベキについても同様に行う。全素数基底のテーブルの値を乗算した計(T)を各 x に対して計算し、次いで $f(x)/T$ を求める。

$f(x)/T$ の値が 1 のものが求める篩結果である。 篩の実施状況を表 2 に示す。

表 2．$f(x)$ の篩による素数基底での分解

x	f(x)	素数基底												累計	f(x)
		-1	2	5	11	17	19	29	41	43	47	61	71	T	/T
-30	4534	1	2	1	1	1	1	1	1	1	1	1	1	2	2267
-29	3895	1	1	5	1	1	19	1	41	1	1	1	1	3895	1
-28	3278	1	2	1	11	1	1	1	1	1	1	1	1	22	149
-27	2683	1	1	1	1	1	1	1	1	1	1	1	1	1	2683
-26	2110	1	2	5	1	1	1	1	1	1	1	1	1	10	211
-25	1559	1	1	1	1	1	1	1	1	1	1	1	1	1	1559
-24	1030	1	2	5	1	1	1	1	1	1	1	1	1	10	103
-23	523	1	1	1	1	1	1	1	1	1	1	1	1	1	523
-22	38	1	2	1	1	1	19	1	1	1	1	1	1	38	1
-21	-425	-1	1	5^2	1	17	1	1	1	1	1	1	1	-425	1
-20	-866	-1	2	1	1	1	1	1	1	1	1	1	1	-2	433
-19	-1285	-1	1	5	1	1	1	1	1	1	1	1	1	-5	257
-18	-1682	-1	2	1	1	1	1	29^2	1	1	1	1	1	-1682	1
-17	-2057	-1	1	1	11^2	17	1	1	1	1	1	1	1	-2057	1
-16	-2410	-1	2	5	1	1	1	1	1	1	1	1	1	-10	241

-15	-2741	-1	1	1	1	1	1	1	1	1	1	1	1	-1	2741
-14	-3050	-1	2	5^2	1	1	1	1	1	1	1	61	1	-3050	1
-13	-3337	-1	1	1	1	1	1	1	1	1	47	1	71	-3337	1
-12	-3602	-1	2	1	1	1	1	1	1	1	1	1	1	-2	1801
-11	-3845	-1	1	5	1	1	1	1	1	1	1	1	1	-5	769
-10	-4066	-1	2	1	1	1	19	1	1	1	1	1	1	-38	107
-9	-4265	-1	1	5	1	1	1	1	1	1	1	1	1	-5	853
-8	-4442	-1	2	1	1	1	1	1	1	1	1	1	1	-2	2221
-7	-4597	-1	1	1	1	1	1	1	1	1	1	1	1	-1	4597
-6	-4730	-1	2	5	11	1	1	1	1	43	1	1	1	-4730	1
-5	-4841	-1	1	1	1	1	1	1	1	1	47	1	1	-47	103
-4	-4930	-1	2	5	1	17	1	29	1	1	1	1	1	-4930	1
-3	-4997	-1	1	1	1	1	19	1	1	1	1	1	1	-19	263
-2	-5042	-1	2	1	1	1	1	1	1	1	1	1	1	-2	2521
-1	-5065	-1	1	5	1	1	1	1	1	1	1	1	1	-5	1013
0	-5066	-1	2	1	1	17	1	1	1	1	1	1	1	-34	149
1	-5045	-1	1	5	1	1	1	1	1	1	1	1	1	-5	1009
2	-5002	-1	2	1	1	1	1	1	41	1	1	61	1	-5002	1
3	-4937	-1	1	1	1	1	1	1	1	1	1	1	1	-1	4937
4	-4850	-1	2	25	1	1	1	1	1	1	1	1	1	-50	97
5	-4741	-1	1	1	11	1	1	1	1	1	1	1	1	-11	431
6	-4610	-1	2	5	1	1	1	1	1	1	1	1	1	-10	461
7	-4457	-1	1	1	1	1	1	1	1	1	1	1	1	-1	4457
8	-4282	-1	2	1	1	1	1	1	1	1	1	1	1	-2	2141
9	-4085	-1	1	5	1	1	19	1	1	43	1	1	1	-4085	1
10	-3866	-1	2	1	1	1	1	1	1	1	1	1	1	-2	1933
11	-3625	-1	1	5^3	1	1	1	29	1	1	1	1	1	-3625	1
12	-3362	-1	2	1	1	1	1	1	41^2	1	1	1	1	-3362	1
13	-3077	-1	1	1	1	17	1	1	1	1	1	1	1	-17	181
14	-2770	-1	2	5	1	1	1	1	1	1	1	1	1	-10	277
15	-2441	-1	1	1	1	1	1	1	1	1	1	1	1	-1	2411
16	-2090	-1	2	5	11	1	19	1	1	1	1	1	1	-2090	1
17	-1717	-1	1	1	1	17	1	1	1	1	1	1	1	-17	101
18	-1322	-1	2	1	1	1	1	1	1	1	1	1	1	-2	661
19	-905	-1	1	5	1	1	1	1	1	1	1	1	1	-5	181
20	-466	-1	2	1	1	1	1	1	1	1	1	1	1	-2	233
21	-5	-1	1	5	1	1	1	1	1	1	1	1	1	-5	1
22	478	-1	2	1	1	1	1	1	1	1	1	1	1	2	239
23	983	-1	1	1	1	1	1	1	1	1	1	1	1	1	983
24	1510	-1	2	5	1	1	1	1	1	1	1	1	1	10	151
25	2059	-1	1	1	1	1	1	29	1	1	1	1	71	2059	1
26	2630	-1	2	5	1	1	1	1	1	1	1	1	1	10	263
27	3223	-1	1	1	11	1	1	1	1	1	1	1	1	11	293
28	3838	-1	2	1	1	1	19	1	1	1	1	1	1	38	101
29	4475	-1	1	5^2	1	1	1	1	1	1	1	1	1	25	179
30	5134	-1	2	1	1	17	1	1	1	1	1	1	1	34	151

(3) 篩結果により作成した行列

表 2 で $f(x)/T$ の値が 1 のものだけ取り出し、$(11x+5)^2 = 11 \cdot f(x)$ の関係を使用し、表 3 の行列を作成する。ここで、素数基底に対応する表の値は素数基底のベキ数を入れる。$(11+5)^2$ は平方数なのでその平方根として $11x+5$ の絶対値を入れる。

表 3．分解関係行列

			素数基底												平方数
No.	x	f(x)	-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

4．因数分解

SISQ による因数分解を参照。