GNFS による篩例(3 次多項式)

2006/03/26　後　保範
2006/11/13　指摘修正

1. 合成数に対応する関数

$N=1333$ を GNFS を使用し基底因子(素数基底と素イデアル基底)で篩を行う。
篩の結果を用いて因数分解するのは GNFS による因数分解を参照。
$f(x)=x^3+2,\quad M=11,\quad f(M)=N$

2. 素数と素イデアルの作成

p を素数とし、 $f(x)=(x-s)g(x) \bmod p$ となる p と s の組を求める。
これは、 $f(s)=0 \bmod p$ より (p,s) の組を求めることに対応する。
下記に $p=31$ までの素数に対応する素イデアル (p,s) の組を示す。

p	2	3	5	7	11	13	17	19	23	29	31
s	0	1	2	---	4	---	-8	---	7	3	-4
	---	---	---	---	---	---	---	---	---	---	-7
	---	---	---	---	---	---	---	---	---	---	11

3. 素数よる篩

(1) 使用する素数と素イデアル

素数 p は 2～19 まで使用し P1～P8 に対応させる。
即ち、P1=2, P2=3, P3=5, P4=7, P5=11, P6=13, P7=17, P8=19 とする。

(2) 素数による篩

$a+bM$ を素数 P1～P8 で完全に分解されたものを選ぶ。
篩は下記の様に行う。実際のプログラムでは各素数に対応するテーブルはメモリを多く必要とするため作成しない。

(a) 表 1 の素数篩のテーブルを 1 に、累計(T)と $(a+Mb)/T$ の欄を 0 に初期化する
(b) $a=-8$～$8, b=1$～5 の範囲で $a+bM=0 \bmod p$ となる位置に p を乗算する。
これは p のベキに付いても実施する。 b が偶数なら a は奇数だけにする。
(c) a,b が互いに素なら GCD の欄に 1 をセットし、それ以外は 0 をセットする。
(d) $a+bM$ の値を計算する。計算は GCD が 1 のところだけ。
(e) 素数基底 P1～P8 に対応するテーブルの値を乗算した累計(T)を各 $a+bM$ に対して計算する。計算は GCD が 1 のところだけ。
(f) GCD=1 の欄に対して $(a+bM)/T$ を計算する。

(3) 素数による篩結果

表 1 に素数による篩結果を示す。$(a+bM)/T=1$のものが求めるものである。

実際の篩では$(a+bM)/T$ の値が 1 だけではなく、適当な基準値以下の値なら候補リストに入れる。この値に同じものが 2 個以上あれば候補リストから篩結果リストに移動する。値が 1 のものは最初から篩結果リストに入れる。

表 1. GNFS による素数篩結果

係数		関数値	採否	素数基底								累計	因子
				2	3	5	7	11	13	17	19		a+bM
a	b	a+bM	GCD	P1	P2	P3	P4	P5	P6	P7	P8	T	/T
-8	1	3	1	1	3	1	1	1	1	1	1	3	1
-7	1	4	1	2^2	1	1	1	1	1	1	1	4	1
-6	1	5	1	1	1	5	1	1	1	1	1	5	1
-5	1	6	1	2	3	1	1	1	1	1	1	6	1
-4	1	7	1	1	1	1	7	1	1	1	1	7	1
-3	1	8	1	2^3	1	1	1	1	1	1	1	8	1
-2	1	9	1	1	3^2	1	1	1	1	1	1	9	1
-1	1	10	1	2	1	5	1	1	1	1	1	10	1
0	1	11	1	1	1	1	1	11	1	1	1	11	1
1	1	12	1	2^2	3	1	1	1	1	1	1	12	1
2	1	13	1	1	1	1	1	1	13	1	1	13	1
3	1	14	1	2	1	1	7	1	1	1	1	14	1
4	1	15	1	1	3	5	1	1	1	1	1	15	1
5	1	16	1	2^4	1	1	1	1	1	1	1	16	1
6	1	17	1	1	1	1	1	1	1	17	1	17	1
7	1	18	1	2	3^2	1	1	1	1	1	1	18	1
8	1	19	1	1	1	1	1	1	1	1	19	19	1
-7	2	15	1	1	3	5	1	1	1	1	1	15	1
-5	2	17	1	1	1	1	1	1	1	17	1	17	1
-3	2	19	1	1	1	1	1	1	1	1	19	19	1
-1	2	21	1	1	3	1	7	1	1	1	1	21	1
1	2	23	1	1	1	1	1	1	1	1	1	1	23
3	2	25	1	1	1	5^2	1	1	1	1	1	25	1
5	2	27	1	1	3^3	1	1	1	1	1	1	27	1
7	2	29	1	1	1	1	1	1	1	1	1	1	29
-8	3	25	1	1	1	5^2	1	1	1	1	1	25	1
-7	3	26	1	2	1	1	1	1	13	1	1	26	1
-6	3	27	0	1	3^3	1	1	1	1	1	1	0	0
-5	3	28	1	2^2	1	1	7	1	1	1	1	28	1
-4	3	29	1	1	1	1	1	1	1	1	1	1	29
-3	3	30	0	2	3	5	1	1	1	1	1	0	0
-2	3	31	1	1	1	1	1	1	1	1	1	1	31
1	3	32	1	2^5	1	1	1	1	1	1	1	32	1
0	3	33	0	1	3	1	1	11	1	1	1	0	0

1	3	34	1	2	1	1	1	1	1	17	1	34	1
2	3	35	1	1	1	5	7	1	1	1	1	35	1
3	3	36	0	2^2	3^2	1	1	1	1	1	1	0	0
4	3	37	1	1	1	1	1	1	1	1	1	1	37
5	3	38	1	2	1	1	1	1	1	1	19	38	1
6	3	39	0	1	3	1	1	1	13	1	1	0	0
7	3	40	1	2^3	1	5	1	1	1	1	1	40	1
8	3	41	1	1	1	1	1	1	1	1	1	1	41
−7	4	37	1	1	1	1	1	1	1	1	1	1	37
−5	4	39	1	1	3	1	1	1	13	1	1	39	1
−3	4	41	1	1	1	1	1	1	1	1	1	1	41
−1	4	43	1	1	1	1	1	1	1	1	1	1	43
1	4	45	1	1	3^2	5	1	1	1	1	1	45	1
3	4	47	1	1	1	1	1	1	1	1	1	1	47
5	4	49	1	1	1	1	7^2	1	1	1	1	49	1
7	4	51	1	1	3	1	1	1	1	17	1	51	1
−8	5	47	1	1	1	1	1	1	1	1	1	1	47
−7	5	48	1	2^4	3	1	1	1	1	1	1	48	1
−6	5	49	1	1	1	1	7^2	1	1	1	1	49	1
−5	5	50	0	2	1	5^2	1	1	1	1	1	0	0
−4	5	51	1	1	3	1	1	1	1	17	1	51	1
−3	5	52	1	2^2	1	1	1	1	13	1	1	52	1
−2	5	53	1	1	1	1	1	1	1	1	1	1	53
−1	5	54	1	2	3^3	1	1	1	1	1	1	54	1
0	5	55	0	1	1	5	1	11	1	1	1	0	0
1	5	56	1	2^3	1	1	7	1	1	1	1	56	1
2	5	57	1	1	3	1	1	1	1	1	19	57	1
3	5	58	1	2	1	1	1	1	1	1	1	2	29
4	5	59	1	1	1	1	1	1	1	1	1	1	59
5	5	60	0	2^2	3	5	1	1	1	1	1	0	0
6	5	61	1	1	1	1	1	1	1	1	1	1	61
7	5	62	1	2	1	1	1	1	1	1	1	2	31
8	5	63	1	1	3^2	1	7	1	1	1	1	63	1

4. 素イデアルによる篩

(1) 使用する素イデアル

素イデアルは分解用(Q)と平方剰余用(R)の 2 種類に分ける。

分解用イデアル Q(p;s)として Q1(2;0),Q2(3;1),Q3(5;2),Q4(11;4),Q5(17;-8),Q6(23;7)を使用する。

平方剰余用イデアル R(p;s)として R1(29;3),R2(31;-7)を使用する。

(2) 素イデアルによる篩

イデアル $a+b\theta$ に対すノルムを $N(a,b)=\left|b^3 f\left(-\frac{a}{b}\right)\right|=\left|a^3-2b^3\right|$ で与える。

$N(a,b)$ がイデアル $a+b\theta$ を素イデアル Qk(p_k;s_k)で分解するには、$N(a,b)$ を p_k

で完全に分解されるものを選ぶ。

$N(a,b)$ が p_k で割れることと、$a+bs_k$ が p_k で割れることは同じであり、高速化のため、まず $a+bs_k$ が p_k で割れる p_k を選び、その p_k で $N(a,b)$ が完全に分解されるかのテストを行う。具体的には下記の様に行う。

(a) 表 2 の素数イデアル篩のテーブルを 1 に、累計(T)と N/T の欄を 0 にする。

(b) 表 2 の有効(Y)の欄に表 1 の $a+bM \ /T$ が 1 なら 1 をそれ以外なら 0 を入れる。

(c) $a=-8\sim8, b=1\sim5$ の範囲で各素イデアル(Q1～Q6)に対して $a+bs=0 \mod p$ となる位置に値 p を乗算する。b が偶数なら a は奇数だけにする。

(d) 有効(Y)の欄が 1 で各素イデアル(Q1～Q6)が 1 以外なら、ノルム $N(a,b)$ が各素イデアルの p のベキで割れるかのテストを行う。k が 2 以上の p^k で割れればその値を対応場所にセットする。

(e) 各 a,b に対して $N(a,b)$ の値を計算する。

(f) 素イデアル基底 Q1～Q6 に対応するテーブルの値を乗算した累計(T)を各 a,b に対して計算する。計算は有効(Y)が 1 のところだけ。

(g) 有効(Y)の欄が 1 なら、$N(a,b)/T$ を計算する。

(3) 素イデアルによる篩結果

表 2 に素イデアルによる篩結果を示す。$N(a,b)/T=1$ のものが求めるものである。 実際の篩では $N(a,b)/T$ の値が 1 だけではなく、適当な基準値以下の値なら候補リストに入れる。この値に同じものが 2 個以上あれば候補リストから篩結果リストに移動する。値が 1 のものは最初から篩結果リストに入れる。

表 2. GNFS による素イデアル篩結果

係数		有効	ノルム	素イデアル基底						累計	因子
			N(a, b)	Q1	Q2	Q3	Q4	Q5	Q6		
			p	2	3	5	11	17	23		N(a, b)
a	b	Y	s	0	1	2	4	-8	7	T	/T
-8	1	1	514	2	1	1	1	1	1	2	257
-7	1	1	345	1	3	5	1	1	23	345	1
-6	1	1	218	2	1	1	1	1	1	2	109
-5	1	1	127	1	1	1	1	1	1	1	127
-4	1	1	66	2	3	1	11	1	1	66	1
-3	1	1	29	1	1	1	1	1	1	1	29
-2	1	1	10	2	1	5	1	1	1	10	1
-1	1	1	3	1	3	1	1	1	1	3	1
0	1	1	2	2	1	1	1	1	1	2	1
1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	6	2	3	1	1	1	1	6	1
3	1	1	25	1	1	25	1	1	1	25	1

4	1	1	62	2	1	1	1	1	1	2	31
5	1	1	123	1	3	1	1	1	1	3	41
6	1	1	214	2	1	1	1	1	1	2	107
7	1	1	341	1	1	1	11	1	1	11	31
8	1	1	510	2	3	5	1	17	1	510	1
−7	2	1	359	1	1	1	1	1	1	1	359
−5	2	1	141	1	3	1	1	1	1	3	47
−3	2	1	43	1	1	1	1	1	1	1	43
−1	2	1	17	1	1	1	1	17	1	17	1
1	2	0	15	1	3	5	1	1	1	0	0
3	2	1	11	1	1	1	11	1	1	11	1
5	2	1	109	1	1	1	1	1	1	1	109
7	2	0	327	1	3	1	1	1	1	0	0
−8	3	1	566	2	1	1	1	1	1	2	283
−7	3	1	397	1	1	1	1	1	1	1	397
−6	3	0	270	2	3	5	1	1	1	0	0
−5	3	1	179	1	1	1	1	1	1	1	179
−4	3	0	118	2	1	1	1	1	1	0	0
−3	3	0	81	1	3	1	1	1	1	0	0
−2	3	0	62	2	1	1	1	1	1	0	0
−1	3	1	55	1	1	5	11	1	1	55	1
0	3	0	54	2	3	1	1	1	1	0	0
1	3	1	53	1	1	1	1	1	1	1	53
2	3	1	46	2	1	1	1	1	23	46	1
3	3	0	27	1	3	1	1	1	1	0	0
4	3	0	10	2	1	5	1	1	1	0	0
5	3	1	71	1	1	1	1	1	1	1	71
6	3	0	162	2	3	1	1	1	1	0	0
7	3	1	289	1	1	1	1	17^2	1	289	1
8	3	0	458	2	1	1	1	1	1	0	0
−7	4	0	471	1	3	1	1	1	1	0	0
−5	4	1	253	1	1	1	11	1	23	253	1
−3	4	0	155	1	1	5	1	1	1	0	0
−1	4	0	129	1	3	1	1	1	1	0	0
1	4	1	127	1	1	1	1	1	1	1	127
3	4	0	101	1	1	1	1	1	1	0	0
5	4	1	3	1	3	1	1	1	1	3	1
7	4	1	215	1	1	5	1	1	1	5	43
−8	5	0	762	2	3	1	1	1	1	0	0
−7	5	1	593	1	1	1	1	1	1	1	593
−6	5	1	466	2	1	1	1	1	1	2	233
−5	5	0	375	1	3	5	1	1	1	0	0
−4	5	1	314	2	1	1	1	1	1	2	157
−3	5	1	277	1	1	1	1	1	1	1	277

-2	5	0	258	2	3	1	1	1	1	0	0
-1	5	1	251	1	1	1	1	1	1	1	251
0	5	0	250	2	1	5	1	1	1	0	0
1	5	1	249	1	3	1	1	1	1	3	83
2	5	1	242	2	1	1	11^2	1	1	242	1
3	5	0	223	1	1	1	1	1	1	0	0
4	5	0	186	2	3	1	1	1	1	0	0
5	5	0	125	1	1	5	1	1	1	0	0
6	5	0	34	2	1	1	1	17	1	0	0
7	5	0	93	1	3	1	1	1	1	0	0
8	5	1	262	2	1	1	1	1	1	2	131

5. 素数と素イデアルの篩結果

(1) 素イデアルによる平方剰余の計算

素数と素イデアルにより共に篩にかかったイデアル$a+b\theta$に対して各 R(p;s)で平方剰余になるか非平方剰余になるか調べ、平方剰余なら 0 を非平方剰余なら 1 とする。平方剰余のテストは$a-bs$が p の平方剰余かどうか、即ち$(a-bs)^{(p-1)/2} \bmod p$を計算し、その結果が 1 なら 0 を-1 なら 1 とする。$a-bs$が p の倍数なら平方剰余で 0 とする。

注）通常は$a+bs$の平方剰余を使用している。$a-bs$でも確率的に同じ。

(2) 篩の結果

表 2 の素イデアル篩において$N(a,b)/T=1$となる項を集めると篩結果となる。

表 3 に篩結果を示す。素数(P1～P8)と素イデアル(Q1～Q5)の欄にはベキ数を入れ、平方剰余(R1,R2)に対応する部分は平方剰余計算式で求めた 0 か 1 を入れる。

表 3. GNFS による篩結果

No	a	b	P1	P2	P3	P4	P5	P6	P7	P8	Q1	Q2	Q3	Q4	Q5	Q6	R1	R2
1	-7	1	2	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0
2	-4	1	0	0	0	1	0	0	0	0	1	1	0	1	0	0	0	1
3	-2	1	0	2	0	0	0	0	0	0	1	0	1	0	0	0	0	0
4	-1	1	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1
5	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
6	1	1	2	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0
7	2	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0
8	3	1	1	0	0	1	0	0	0	0	0	0	2	0	0	0	0	0
9	8	1	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	1
10	-1	2	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1
11	3	2	0	0	2	0	0	0	0	0	0	0	0	1	0	0	1	1
12	-1	3	5	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0

13	2	3	0	0	1	1	0	0	0	0	1	0	0	0	0	1	0	1
14	7	3	3	0	1	0	0	0	0	0	0	0	0	0	2	0	1	0
15	−5	4	0	1	0	0	0	1	0	0	0	0	0	1	0	1	1	1
16	5	4	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	0
17	2	5	0	1	0	0	0	0	0	1	1	0	0	2	0	0	0	1

6. GNFS による因数分解

   GNFS による因数分解例を参照。