岡山大学算数・数学教育学会誌
『パピルス』第３号（1996年）69頁～75頁

Number Field Sieveによる素因数分解とその計算機実験

加藤　慎一
岡山大学大学院教育学研究科

近年，コンピューターを使用して色々な巨大数の素因数分解の方法が研究されている。本論は，現在その中で最も可能性があるNumber Field Sieve (以下NFS)のアルゴリズムを利用し，パソコン上で動くFORTRAN言語であるMicrosoft FORTRAN Ver.5.1を用い，$n=2^{5k}-3,(k=1,2,\cdots)$の形をした自然数の素因数分解を，50桁を目標として試み，その有用性，限界を確かめ，改良を試みたものである。

1．NFSのための準備

自然数$n=2^{5k}-3$の素因数分解を行うため，５次多項式$f(X)=X^5-3$を導入する。そして，$f(X)=0$の根$\sqrt[5]{3}$を有理数体$\mathbf{Q}$に添加した５次体$F=\mathbf{Q}(\sqrt[5]{3})$を考える。このとき体$F$の元$\sum_{i=0}^{4} r_i \sqrt[5]{3}^{\,i}$で$r_i \in \mathbf{Z}$で構成される整数環を$\mathbf{Z}[\sqrt[5]{3}]$とする。このとき$F$の全整数環$\mathbf{O}_F$と$\mathbf{Z}[\sqrt[5]{3}]$が一致すること，即ち指数$m=(\mathbf{O}_F:\mathbf{Z}[\sqrt[5]{3}])=1$であることがアイゼンシュタインの定理の系により示される。

また，体Fの判別式を$d(F)$，５次多項式$f(X)=X^5-3$の判別式を$D(f)$とすると$D(f)=5^5\cdot 3^4$であることが計算でき，$D(f)=m^2\cdot d(F)$より，$D(f)=d(F)=5^5\cdot 3^4$となることがわかる。さらに，体Fの判別式$d(F)=5^5\cdot 3^4$を利用して，ミンコフスキー定数が$M_F<31.4$となることが計算できる。

よって，ミンコフスキーの定理の系から31以下のノルムをもつ１次の素イデアル$\mathfrak{p}$，または$p\le 31$の上にある素イデアルについてそれらが全て単項イデアルであることを計算することにより$\mathbf{Q}(\sqrt[5]{3})$の類数が１であることが確かめられる。よって，全整数環$\mathbf{Z}[\sqrt[5]{3}]$が単項イデアル整域となる。

即ち，$\mathbf{Z}[\sqrt[5]{3}]$の全ての素イデアル$\mathfrak{p}$に対して，$\pi_{\mathfrak{p}} \in \mathbf{Z}[\sqrt[5]{3}]$を$\mathfrak{p}=\pi_{\mathfrak{p}}\mathbf{Z}[\sqrt[5]{3}]$となるように選ぶことができる。この$\pi_{\mathfrak{p}}$を素イデアル$\mathfrak{p}$の生成元とよぶ。

また，整数環$\mathbf{Z}[\sqrt[5]{3}]$から有限体$\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$（$p$は素数）への環準同型を$c\in\mathbf{F}_p$で$c^5\equiv 3\ (mod\ p)$となる元を対応させることにより次のように定義できる。

$$\psi_{p,c}(\sqrt[5]{3})=(c \bmod p),(c^5\equiv 3 \bmod p)$$

この写像により1次の素イデアル$\mathfrak{p}$は整数の組(p,c)に対応しており，pと$c-\sqrt[3]{3}$とで生成されたイデアルとなる。そして，その生成元$\pi_{\mathfrak{p}} \in \mathbf{Z}[\sqrt[3]{3}]$はこの環準同型$\psi_{p,c}$により次の(i),(ii)ように決定できる。

(i) $p \not\equiv 1 (mod\ 5)$のとき，素数pに対して整数の組(p,c)はただ1通りしか存在せず，このとき1次の素イデアル$\mathfrak{p}$と(p,c)は$\psi_{p,c}$により1対1に対応する。このとき$\pi \in \mathbf{Z}[\sqrt[3]{3}]$でノルムの絶対値が$|N(\pi)| = p$となるものが生成元$\pi_{\mathfrak{p}}$である。

(ii) $p \equiv 1 (mod\ 5)$のとき，ペアが全く現れないか，5つ現れるかのいずれかになる。5つ現れるとき各々の1次の素イデアル$\mathfrak{p}$と(p,c)は1対1で対応する。このとき$\pi \in \mathbf{Z}[\sqrt[3]{3}]$でノルムの絶対値が$|N(\pi)| = p$であり，$\psi_{p,c}(\pi) = 0 (mod\ p)$となるものが生成元$\pi_{\mathfrak{p}}$となる。

また，単項イデアル整域は一意分解整域であるので，$\mathbf{Z}[\sqrt[3]{3}]$の0でない元βは1次の素イデアル$\mathfrak{p}$の生成元$\pi_{\mathfrak{p}} \in \mathbf{Z}[\sqrt[3]{3}]$で単数$\varepsilon$を除いて一意的に分解される。このとき，$0 \neq \beta \in \mathbf{Z}[\sqrt[3]{3}]$に対して負でない整数$e(\mathfrak{p})$が一意的に決定し

$$\beta = \varepsilon \cdot \prod_{\mathfrak{p}} \pi_{\mathfrak{p}}^{e(\mathfrak{p})}$$

とかける。ここでβのノルムを考え環準同型$\psi_{p,c}$を利用すればべき$e(\mathfrak{p})$を決定できる。

また，εは$\mathbf{Z}[\sqrt[3]{3}]$の単数群$\mathbf{Z}[\sqrt[3]{3}]^*$に含まれる。単数群$\mathbf{Z}[\sqrt[3]{3}]^*$は1のべき根

$$\varepsilon_0 = -1$$

と2つの基本単数

$$\varepsilon_1 = 1 + \sqrt[3]{3} + \sqrt[3]{3}^3$$

$$\varepsilon_2 = 4 + 2\sqrt[3]{3} + \sqrt[3]{3}^4$$

で生成され，

$$\varepsilon = \prod_{i=0}^{2} \varepsilon_i^{e(i)},\ e(0) \in \mathbf{Z}/2\mathbf{Z},\ e(1), e(2) \in \mathbf{Z}$$

と分解できる。このべき$e(i), (0 \le i \le 2)$の決定は[1, 4.17]の方法を利用できる。

2. NFSのアウトライン

簡単な例で考えてみる。$n = 2^{5k} - 3$のとき，

$$2^{5k} = (2^k)^5 \equiv 3 (mod\ n)$$

より，整数環$\mathbf{Z}[\sqrt[3]{3}]$から$\mathbf{Z}/n\mathbf{Z}$への環準同型φを

$$\varphi(\sqrt[3]{3}) = (2^k\ mod\ n)$$

で定義できる。

ここで$\gcd(a,b) = 1$となる有理整数a, bに対して，

・有理整数$a + 2^k b$が$\mathbf{Z}$で平方数

・代数的整数$a + b\sqrt[3]{3}$が整数環$\mathbf{Z}[\sqrt[3]{3}]$において平方数

と仮定する。即ち，

$$a + 2^k b = x^2,\ a + b\sqrt[3]{3} = \beta^2$$

と表せる。環準同型φにより次の2つの等式が成立する。（ただし$y \equiv \varphi(\beta)\ (mod\ n)$とする。）

$$\varphi(a + b\sqrt[3]{3}) \equiv a + 2^k b = x^2\ (mod\ n)$$

$$\varphi(a + b\sqrt[3]{3}) = \varphi(\beta^2) = \varphi(\beta)^2 \equiv y^2\ (mod\ n)$$

これにより，

$$x^2 \equiv y^2\ (mod\ n)$$

となり，もし

$$x \not\equiv \pm y\ (mod\ n)$$

であれば，

$$\gcd(x+y, n), \gcd(x-y, n)$$

はnの自明でない約数である。

このようにペア(a,b)を見つけるのは不可能であるが，3.で述べるfactor baseを用いることにより$x^2 \equiv y^2$の関係式を導くことができる。

3. NFSのアイデア

NFSは次の３つのStepで構成されている。ここでは今回利用したアルゴリズムに関してのみ記述する。

まず，準備として$B-smooth$について定義する。Bを正の整数とする。このとき，

$$A \in \mathbf{Z}\text{が}B-smooth$$
$$\Leftrightarrow A\text{の素因子がすべて}B\text{以下}$$
$$\text{代数的整数}\alpha \in \mathbf{Z}[\sqrt[3]{3}]\text{が}B-smooth$$
$$\Leftrightarrow \alpha\text{のノルム}N(\alpha)\text{が}B-smooth$$

と定義する。

Step 1　ある適当な上限$B_1, B_2 > 0$を定め，$\gcd(a,b)=1$となる整数a,bに対して，整数$a+2^k b$が$B_1-smooth$，代数的整数$a+b\sqrt[3]{3}$のノルム$N(a+b\sqrt[3]{3})=a^5+3b^5$が$B_2-smooth$であるように選ぶ。

このとき，2.で定義した環準同型φにより

$$\varphi(a+b\sqrt[3]{3}) \equiv a+2^k b \ (mod\ n)$$

となる。また集合P, U, Gを次のように定義し，$I=P\cup U\cup G$とし，この集合Iの元をfactor baseと呼ぶ。

$P\cdots B_1$以下の全ての素数の集合。

$U\cdots\mathbf{Z}[\sqrt[3]{3}]$の単数群$\mathbf{Z}[\sqrt[3]{3}]^*$の生成元の集合。即ち1.における単数$\varepsilon_0, \varepsilon_1, \varepsilon_2$の集合。

$G\cdots\pi_{\mathfrak{p}} \in \mathbf{Z}[\sqrt[3]{3}]$からなる集合。$\pi_{\mathfrak{p}}$は$\mathbf{Z}[\sqrt[3]{3}]$の一次の素イデアル$\mathfrak{p}$の生成元でイデアルのノルムが$B_2$以下の範囲にあるもの。

1.によりこの生成元も全て決定できる。

Step 2　次の３つの条件(i),(ii),(iii)を満たす整数のペア(a,b)を探していく$(b>0)$。そのためにB_3を新しく追加の上限として選んでおく。

(i) $\gcd(a,b)=1$

(ii) $|a+2^k b|$は$B_1 < p_1 < B_3$となる素因数p_1を高々１つを除いて$B_1-smooth$である。

(iii) $\left|N(a+b\sqrt[3]{3})\right| = |a^5+3b^5|$は$B_2-smooth$である。

ここでもし$a+2^k b<0$が起こった場合，(a,b)のペアを$(-a,-b)$のペアで置き換えておく。(ii)における素数p_1をlarge primeとよぶ。もし，(ii)においてlarge primeが現れなければ$p_1=1$とする。$p_1=1$に対するペア(a,b)をfull relation，$p_1\neq 1$に対するペア(a,b)をpartial-full relationとよぶ。

次に，簡単のため，(a,b)がfull relationであるとする。(ii)より

$$a+2^k b=\prod_{p\le B_1} p^{e(p)} \quad , e(p)\in \mathbf{Z}_{\ge 0}$$

とかける。また，$a+b\sqrt[3]{3}$は１次の素イデアル$\mathfrak{p}$の生成元$\pi_{\mathfrak{p}} \in G$のいくつかのべきと$\mathbf{Z}[\sqrt[3]{3}]$の単数の積の形で表せる。具体的には，$\left|N(a+b\sqrt[3]{3})\right| = |a^5+3b^5|$の素因数分解を考えることにより決定する。そして，単数はUの元$\varepsilon_0, \varepsilon_1, \varepsilon_2$のべきの積で表せる。結果として次のような形を得る。

$$a+b\sqrt[3]{3} = \prod_{i=0}^{2} \varepsilon_i^{e(\varepsilon_i)} \cdot \prod_{N(\pi_{\mathfrak{p}})\le B_2} \pi_{\mathfrak{p}}^{e(\mathfrak{p})}$$

$$e(\varepsilon_0)\in \mathbf{Z}/2\mathbf{Z},\ e(\varepsilon_1), e(\varepsilon_2)\in \mathbf{Z},\ e(\mathfrak{p})\in \mathbf{Z}_{\ge}$$

ここで，$a+2^k b$と$a+b\sqrt[3]{3}$は同じ準同型写像φの下で考えられるので，

$$\varphi(a+2^k b) \equiv a+2^k t$$
$$\equiv \prod_{p\le B_1} \varphi(p)^{e(p)} \ (mod\ n)$$

$$\varphi(a+b\sqrt[3]{3}) \equiv a+2^k b$$
$$\equiv \prod_{i=0}^{2} \varphi(\varepsilon_i)^{e(\varepsilon_i)} \cdot \prod_{N(\pi_\mathbf{p})\le B_2} \varphi(\pi_\mathbf{p})^{e(\mathbf{p})} \quad (mod\ n)$$

により次の関係式が導かれる。

$$\prod_{p\le B_1} \varphi(p)^{e(p)}$$
$$\equiv \prod_{i=0}^{2} \varphi(\varepsilon_i)^{e(\varepsilon_i)} \cdot \prod_{N(\pi_\mathbf{p})\le B_2} \varphi(\pi_\mathbf{p})^{e(\mathbf{p})} \quad (mod\ n)$$

Step 3 次にfactor baseの個数を$M=|U|+|G|+|P|$，full relationの個数をNとする。そしてi番目のfull relationのfactor baseのべき$e(\varepsilon_i), e(\mathbf{p}), e(p)$の値を順番に$f_{i1}, f_{i2}, \cdots, f_{iM}$とし，ベクトル

$$\mathbf{f}_i = (f_{i1}, f_{i2}, \cdots, f_{iM}),\ (1 \le i \le N)$$

とする。そしてベクトル$\mathbf{f}_i$の各成分

$$f_{ij}, (1 \le i \le N, 1 \le j \le M)$$

に対して，

$$e_{ij} \equiv f_{ij}, (mod\ 2)$$

と定義し，ベクトル

$$\mathbf{e}_i = (e_{i1}, e_{i2}, \cdots, e_{iM}), (1 \le i \le N)$$

を考える。もしfull relationを$M+1$個見つけることができればベクトル

$$\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_M, \mathbf{e}_{M+1}$$

には$mod\ 2$で1次従属の関係がある。即ち，

$$a_1\mathbf{e}_1 + \cdots + a_M\mathbf{e}_M + a_{M+1}\mathbf{e}_{M+1} \equiv \mathbf{0}\ (mod\ 2)$$

となる

$$a_1, a_2, \cdots, a_{M+1} \in \mathbf{Z/2Z}$$

が存在する。

このとき$a_1, a_2, \cdots, a_{M+1}$に対してベクトル

$$\mathbf{f} = a_1\mathbf{f}_1 + a_2\mathbf{f}_2 + \cdots + a_M\mathbf{f}_M + a_{M+1}\mathbf{f}_{M+1}$$

の各成分は全て偶数となる。よって，full relationの積をこの結合に従ってとると，factor baseのべきを全て偶数にできる。

具体的にはベクトル$\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_M, \mathbf{e}_{M+1}$からつくられる行列

$$(\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_M, \mathbf{e}_{M+1})$$

を$\mathbf{Z/2Z}$上で掃き出し法を用いて計算すればよい。このようにして，full relationを選び，積を考え，そのべきを全て偶数にできる。このとき，

$$x \equiv \prod_{p\in P} \varphi(p)^{\frac{\sum(e(p))}{2}} \equiv \prod_{p\in P} p^{\frac{\sum(e(p))}{2}} \quad (mod\ n)$$

$$y \equiv \prod_{i=0}^{2} \varphi(\varepsilon_i)^{\frac{\sum e(\varepsilon_i)}{2}} \cdot \prod_{N(\pi_\mathbf{p})\le B_2} \varphi(\pi_\mathbf{p})^{\frac{\sum e(\mathbf{p})}{2}} \quad (mod\ n)$$

とすれば

$$x^2 \equiv y^2\ (mod\ n)$$

となる。もし

$$x \not\equiv \pm y\ (mod\ n)$$

であれば

$$\gcd(x+y, n),\ \gcd(x-y, n)$$

がnの約数になる。また，同じlarge prime p_1をもつpertial-full relationの組を見つけることができれば，この組のfactor baseのべきの和をとり，full relationと同様に利用することができる。以上がNFSのアイデアである。

4．実験結果

素因数分解の結果は次の表の通り。

（ただし，$k=1,\cdots,8$はNFSを利用していない。）

$2^{5k}-3,(k=1,2,\cdots)$		
k	digits	factors
1	2	29
2	4	1021
3	5	5 · 6553
4	7	1048573
5	8	479 · 70051
6	10	23 · 46684427
7	11	5 · 6871947673
8	13	13 · 84577817521
9	14	2087 · 48193 · 349819
10	16	59 · 176329 · 108224111
11	17	5 · 1871 · 2207 · 2621 · 665789
12	19	1177067 · 979486728119
13	20	47 · 239831 · 3273004044197
14	22	107 · 3096609167 · 3563112409
15	23	5 · 619 · 2151491857 · 5673477211
16	25	647 · 9277 · 429181 · 469296514307
17	26	19 · 23 · 2854823137 · 31009087508041
18	28	1823 · 735556271 · 923202642033037
19	29	5 · 7922816251426433759354395033
20	31	13 · 419 · 232724545663343014778172059
21	32	67 · 577 · 61845503 · 16966443015568478977
22	34	743 · 10607 · 2424173639 · 67944517065563939

また，分解に使用した各数値データを次の表にまとめる。

表1　分解結果1

共通データ1

$a_{max} = -a_{min}$	b_{max}	B_2	$\#(B_2 - smooth)$
500	500	10000	8130

ペア(a,b)のa,bの動く範囲…$a_{min} \le a \le a_{max}$，$1 \le b \le b_{max}$

$\#(B_2 - smooth)$…上のa,bの範囲で(a,b)=1，$B_2 - smooth$となるペア(a,b)の個数

上の範囲のペア(a,b)に対してfull relationのみで分解できるのは次の通り。

k	digits	$B_1 = B_2$	$\#U+\#G+\#P$	factor base size	ff
9	14	1000	3+153+168	324	325
10	16				325
11	17				312
12	19	2000	3+290+303	596	597
13	20				597
14	22				594
15	23	3000	3+437+430	870	871
16	25				789
17	26	4000	3+551+550	1104	1102
		5000	3+671+669	1343	
18	28	6000	3+769+783	1555	1432
19	29	7000	3+909+900	1812	1623
		8000	3+1011+1007	2021	
		9000	3+1104+1117	2224	
		10000	3+1208+1229	2440	

具体的には次の手順で分解を試みた。

1000-*smooth*から分解を試み，分解できればkの値を１つ上げ，おなじ上限で分解を試みる。もし分解できなければ*smooth*の上限を1000ずつ上げていく。その結果が上の表である。参考として利用しなかった*smooth*の上限に関するデータも表にまとめている（空白部分）。

さらに，a,bの範囲を広げ分解を試みた。また，pertial-full relationも使用した。その結果は次の通り。

表2　分解結果2

共通データ2

$a_{max} = -a_{min}$	b_{max}	B_2	$\#(B_2 - smooth)$	$B_1 = B_2$	$\#U+\#G+\#P$	factor base size
1000	500	10000	10451	10000	3+1208+1229	2440

k	digits	B_3	ff	pf	pf's	ff+pf's
20	31		2441			
21	32		2232			
22	34	1000000	1876	3846	246	2122

pf…partial-full relationの個数。

pf's…partial-full relationにおいてlarge prime p_1が同じになる組合せの個数。

bの範囲はそのままでaの範囲を広げた。これにより10451-8130=2321個$B_2 - smooth$となるrelationが増えた。これにより，k=20,21はfull relationのみで分解できた。しかし，k=22の場合，full relationのみでは分解不可能であり，pertial-full relationを利用することにより分解に成功した。

5．結果の分析と今後の課題

今回の実験結果としては小さな素数で34桁の自然数の分解が可能であるという部分でNFSは他の素因数分解方法に対して有用性があると考えられる。ただし，分解の上限を10000に押さえてしまったため目標である50桁の分解は達成できなかった。

また，今後の課題としては次の2つが挙げられる。

1つ目はデータ出力に関する時間の短縮である。今回の実験において最も時間がかかったのは$a+b\sqrt[3]{3}$のノルムの素因数分解の部分である。これを短くするにはsmooth testの改善が挙げられる[2, 4]。

2つ目は分解する数値の桁数を上げていくことである。今回の実験では$k=22$の場合，即ち34桁の自然数までしか分解できなかった。10000-*smooth*ではこの桁数が限界であると考えられる。さらに桁数を上げていくには*smooth*の上限をあげていくことが有効であると考えられる。

主要参考文献

[1] A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, J.M. Pollard, The factorization of the ninth Fermat number, Math. Comp. 61, 1993, pp.319-349.

[2] A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, J.M. Pollard, The number field sieve, The development of the number field sieve, A.K. Lenstra and H.W. Lenstra, Jr., eds., Lecture Notes in Math. 1554, Springer-Verlag, Berlin, 1993, pp.11-42.

（平成8年3月29日受理）