NAS2006(2006/6/13～15)予稿

多数桁数因数分解における多重基底多項式篩

後　保範(早稲田大学)

Multiple Base Polynomial Sieve for Multiple Precision Integer Factorization

Yasunori Ushiro (Waseda University)

MPQS や GNFS に代わる因数分解の方式を提案する。提案方式は 2～4 次の多項式を使用し、篩には素数と一次式の 2 つの基底を使用する。

I propose the factorization method to take the place of MPQS and GNFS. The proposal method based on the 2-4th order polynomials and the sieve uses the two bases of the prime numbers and the linear expressions.

1. はじめに

RSA 暗号や電子認証は多数桁数での因数分解の困難性を利用している。現在知られている手法では、1024 ビットの RSA 暗号の解読はスーパーコンでも数千年かかると予想される。巨大な数の因数分解には QS(Quadratic Sieve、2 次篩法)と GNFS(General Number Field Sieve、一般数体篩法)がある。10 進 100 桁程度までは QS が高速で、それ以上の桁数では GNFS が高速になる。本発表では、QS の一つである MPQS(Multiple Polynomial QS、複数多項式 2 次篩法)や GNFS に代わる因数分解の方式を提案する。この提案方式を多重基底多項式篩法(Multiple Base Polynomial Sieve、以下 MBPS と略す) と名付ける。今回報告する MBPS は 2～4 次の多項式を使用し、篩は素数と一次式の 2 種類の基底を使用する。使用する多項式の次数により適用方法が少し異なる。本発表では、適用方法の検討が進んでいる 3 次多項式と、2 次多項式による MBPS について述べる。なお MBPS は複数の多項式の利用及び、GNFS と結合した 3 種類の基底の利用も可能な方法である。

2. 篩法

合成数を N とするとき、特定の整数 a,b に対して $a^2-b^2=(a-b)(a+b)\equiv 0 \pmod N$の関係を導いて、N を因数分解する方法である。整数 a,b は篩で得られた多数の式の素数のベキ数を、偶数にする組合せの乗算で得られる。

2.1　2 次篩法(QS)

合成数 N に対して、X を $N^{1/2}$ に一番近い整数とし、$(X+k)^2-N=A_k,(k=0,1,2,\cdots)$を計算する。次に、適当な素数の集合 P で A_k が分解されるものを集合 P の要素より多く集める。集めたものから掛け合わせることで、各素数のベキが偶数になる組合せを取り出す。この組合せによる A_k の乗算は素数の乗算の 2 乗になる。従って、$a^2-b^2\equiv 0 \pmod N$が得られる。MPQS は平方式に適当な変換を行う。代表的な変換として、$d^2-N\equiv 0 \pmod c$となる複数の整数(c,d)の組と

整数 x の 2 次式 f(x)を使用して$(cx+d)^2-N=cf(x)$と変換し、f(x)の値を素数基底で分解する。このとき、素数基底は N の平方剰余となる素数だけで構成できる。

2.2　一般数体篩法(GNFS)

合成数 N に対して、f(M)≡0 (mod N)なる多項式を求め、f(x)=0 の根の一つを θ とする。このとき、a+bM を素数基底で分解し、a+b θ を素元と単元で分解したものを集め、その分解の違いを利用する。例えば、N=1333, $f(x)=x^3+2$, f(M)= N, M=11 の例では 2+M=13 と 2+ θ = $\theta(1-\theta)(1+\theta)$から$-10\cdot11\cdot12\equiv13$ (mod N)の関係を得る。これを、分解に利用した素数基底と生成元(素元と単元)の数以上集める。しかし、実際に生成元が得られるのは f(x)が特別な場合だけである。GNFS では、素元で分解する代りに対応する素イデアルで分解する。更に、求めたイデアルの積が平方になる確率を高めるため、イデアルに対する平方剰余を追加する。また、イデアル側はそのままでは平方の形にならないので、根と係数の関係から連立非線形方程式を作成して、平方イデアルの係数を求める。

3. 3 次多項式による MBPS

合成数 N に対して 3 次多項式 $f(x)=Ax^3+Bx^2+Cx+D$ が、f(M)≡0 (mod N)となる整数 A,B,C,D,M を求める。このとき、A,B,C,D の絶対値は小さいものが良い。次に g(x)が一次関数となるよう下記で定義する。

$g(x) = (Ax+a)(x+b)(x+c) - f(x) = sx+t$

$a+A(b+c) = B,\quad s = a(b+c)+Abc - C,\quad t = abc - D$

このようにすると、$(AM+a)(M+b)(M+c)\equiv sM+t$ (mod N)の関係が成立する。篩の基底は、素数と M の一次式により構成する。素数基底は、-1 及び小さい素数から順に選定する。一次式基底は小さい整数 α, β に対して AM+ α 及び M+ β の形で、発生頻度が高い順に選定する。s の絶対値が一定値以下となるよう整数 b,c を動かすと、整数 a は $a=B-A(b+c)$の制約条件で決まる。各 a,b,c に対して、この式の右辺及び左辺を素数基底と一次式基底で篩を行い、両辺がこれらで分解できるものを選び出す。これを、2 種類の基底の合計数より少し多く集める。その後の処理は、MPQS と同様にする。最終的には、一次式は M の値を代入し整数にする。また、f(x)は複数の異なる多項式が使用できる。更に、3 次多項式の最高次の係数 A が整数の積となる場合は、g(x)の作成において A は各一次式に分配でき、1 個の f(x)に対して、g(x)は複数作成できる。

4. 2 次多項式による MBPS

合成数 N に対して 2 次多項式 $f(x)=Ax^2+Bx+C$ が、f(M)≡0 (mod N)となる整数 A,B,C,M を求める。このとき、A,B,C の絶対値は小さいものが良い。次に g(x)が一次関数となるよう下記で定義する。

$g(x) = (Acx+a)(dx+b) - cdf(x) = sx+t$

$s = ad+(Ab-Bd)c,\quad t = ab- Ccd$

このようにすると、$(AcM+a)(dM+b)\equiv sM+t$ (mod N)の関係が成立する。篩のための基底は、素数と M の一次式により構成する。素数基底は、-1 及び小さい素数から順に選定する。一次

式基底は小さい整数 α , β に対して AcM+ α 及び dM+ β の形で、発生頻度が高い順に選定する。s の絶対値が一定値以下となるよう整数 a,b,c および d を動かし、この式の右辺及び左辺を素数基底と一次式基底で篩を行い、両辺がこれらで分解できるものを選び出す。これを、2 種類の基底の合計数より少し多く集める。その後の処理は、MPQS と同様にする。最終的には、一次式は M の値を代入し整数にする。2 次多項式による MBPS も 3 次多項式と処理が似ているが、右辺 sM+t が左辺の一次式と同一なものが発生する比率は、2 次多項式の方が圧倒的に高い。そのため、右辺を一次式基底で分解できる可能性が大きくなる。また、MBPS と GNFS で同一の f(x)を使用することで、同じ一次式基底を用いた篩が可能となる。このため、10 進 100 桁程度以上で GNFS より高速にできる可能性は、2 次多項式による MBPS の方が有望である。但し、共通一次式で結合して作成した式が、既に選定した式と一致する場合が存在する。このため、同一式となるものを削除する手順を入れないと、因数分解結果に自明解の割合が多くなる。

5. 2 次多項式による因数分解例

N=55751 を 2 次式の MBPS により因数分解する例を示す。複数の多項式を利用することができるが、説明を簡単にするために多項式 f(x)は、下記の 1 個だけを使用する。

$f(x) = 2x^2 - 27$,　M=167

c,d が共に 1 でかつ a,b,s の絶対値が 9 以下のもので篩を行う。素数基底は-1 と 2～23 までの 9 個の素数の合計 10 個を使用する。一次式基底は M-3,M,2M+1,2M+3 及び 2M+5 の 5 個を使用する。また、M+1,M+3 等は素数基底で、$M+1=168=2^3\cdot3\cdot7$, $M+3=170=2\cdot5\cdot17$ と分解できるため、表 1 では M の一次式ではなく素数基底に分解して掲載する。素数と一次式の基底の合計は 15 個となるので、篩の結果はそれより 7 個多く 22 個を選定した。表 1 に篩結果の行列を示す。表 1 の正のベキは左辺での指数を、負のベキは右辺での指数を示す。従って、表 1 の No.1～No.4 は(mod N)の基で下記の等式を示す。No.5 以下も同様である。

No.1：　$2M(M+3) \equiv 3(2M+9) \rightarrow 2^2\cdot5\cdot17\cdot M \equiv 3\cdot7^3$

No.2：　$2M(M+1) \equiv 2M+27 \rightarrow 2^4\cdot3\cdot7\cdot M \equiv 19^2$

No.3：　$2M^2 \equiv 27 \rightarrow 2\cdot M^2 \equiv 3^3$

No.4：　$2M(M-3) \equiv -3(2M-9) \rightarrow 2\cdot(M-3)\cdot M \equiv -1\cdot3\cdot5^2\cdot13$

表 1 の B1,B2,B3,B4,B5 はそれぞれ一次式基底 M-3,M,2M+1,2M+3 及び 2M+5 を示す。

表 1. 2 次の MBPS による篩結果の行列（c,d=1）

No	g(x)の係数		mod N での等式														
			素数基底										一次式基底				
	a	b	-1	2	3	5	7	11	13	17	19	23	B1	B2	B3	B4	B5
1	0	3	0	2	-1	1	-3	0	0	1	0	0	0	1	0	0	0
2	0	1	0	4	1	0	1	0	0	0	-2	0	0	1	0	0	0
3	0	0	0	1	-3	0	0	0	0	0	0	0	0	2	0	0	0
4	0	-3	1	1	-1	-2	0	0	-1	0	0	0	1	1	0	0	0
5	1	2	0	-5	-3	0	0	0	2	0	0	0	0	0	1	0	0

6	1	1	0	3	1	0	1	0	0	0	0	-2	0	0	1	0	0
7	1	-2	1	-2	1	1	-1	1	0	-1	0	0	0	0	1	0	0
8	3	3	0	1	-4	1	0	0	0	1	-1	0	0	0	0	1	0
9	3	0	0	-4	-1	0	0	-1	0	0	0	0	0	1	0	1	0
10	3	-3	1	0	-1	0	-1	0	0	0	0	-1	1	0	0	1	0
11	4	-2	0	1	1	1	0	1	2	0	-1	0	0	0	0	0	0
12	5	2	0	-2	0	-1	-1	-1	2	0	0	0	0	0	0	0	1
13	5	-2	0	-3	1	1	0	1	0	0	0	-1	0	0	0	0	1
14	5	-5	1	1	4	0	-2	0	0	-1	0	0	0	0	0	0	1
15	6	-3	0	2	-2	1	0	0	0	1	0	0	1	0	0	0	0
16	6	-6	1	2	-1	1	1	0	0	1	0	1	0	0	0	-1	0
17	9	0	0	-1	-2	-1	3	0	0	-1	0	0	0	1	0	0	0
18	9	-3	0	0	-1	0	3	0	0	0	0	0	1	-1	0	0	0
19	9	-6	1	-4	-1	0	4	-1	0	0	0	1	0	0	0	0	0
20	-9	9	0	4	-2	2	-1	1	1	0	0	-1	0	0	0	0	0
21	-9	4	1	-4	2	2	0	-1	1	0	1	0	0	0	0	0	0
22	-9	3	1	1	-1	3	0	0	1	1	0	0	0	-1	0	0	0

平方式は、表 1 の No.が(5,7,12,14)や(2,5,7,9,10,12,13,15)等の 7 個の組合せが得られる。(5,7,12,14)の組合せから$(3\cdot13^2\cdot335\cdot339)^2\equiv(2^4\cdot7^2\cdot17)^2$ が得られ、(2,5,7,9,10,12,13,15)の組合せから$(5\cdot13^2\cdot164\cdot167\cdot335\cdot337\cdot339)^2\equiv(2^5\cdot3^2\cdot7\cdot19\cdot23)^2$ が得られる。いずれも(mod N)の基での等式である。これより、表1から(mod N)の基で下記の 7 個の平方式が得られる。

$13328^2\equiv13328^2$, $24042^2\equiv11024^2$, $11477^2\equiv1824^2$, $24042^2\equiv11024^2$, $24042^2\equiv11024^2$, $11477^2\equiv1824^2$, $13041^2\equiv13041^2$

最初と最後の式は自明解であるが、他の 5 個の式から、GCD(24042+11024,N)=197、GCD(24042-11024,N)=283 のようにして、N=197·283 と因数分解される。

6. おわりに

提案した多重基底多項式篩法(MBPS)は、QS と同じ多項式篩法の系列であるが、2 乗の壁(素数基底で分解する数が元の数の平方根以下にできない)を、一次式の基底化により除くことができた。そのため、今後の工夫により GNFS に匹敵するか、又は超える可能性がある。今後、計算量推定式の算出及び数値実験によりその実用性を評価する。

謝辞

GNFS の基礎を教えて頂いた立教大学の木田祐司教授と、貴重なコメントを頂いた東京大学の金田康正教授及び、金田研究室の吉田仁氏に謹んで感謝の意を表する。

参考文献

1)木田祐司:初等整数論、朝倉書房 (2003).

2) N.コブリッツ、櫻井幸一訳:数論アルゴリズムと楕円暗号理論入門、Springer (1998).

3)木田祐司:Number Field Sieve(数体篩法) について、木田祐司 HP、http://www.rkmath.rikkyo.ac.jp/~kida/bunkai.htm (1999).

4)後 保範: 多項式篩法(PS, Polynomial Sieve) in RSA 暗号、後 保範 HP、http://ushiro.jp/RSA.htm (2006).