ベクトル計算機による代数的数の平方根の計算方法

後　保範（早稲田大学）

Computation method for square root of algebraic numbers by vector computer.

Yasunori Ushiro (Waseda University)

1. はじめに

RSA 暗号は現在の情報社会において欠かせない技術である。また、現在使用している 1024 ビットの RSA 暗号が安全性の問題で近いうちに使えなくなるという「2010 年問題」が懸念されている。RSA 暗号は多数桁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数十年かかると予想されているが、計算機の高速化により数年先には解読される可能性が高くなっている。2010 年 1 月に NTT 他 4 カ国の共同により、Opteron(2.2GHz)換算で約 1700 年・コアの演算量を使用して RSA-768(10 進 232 桁)が解読された。RSA 暗号の解読計算はほとんど PC クラスタで行われている。

2. RSA 暗号

インターネットで情報を安全に送るために、暗号化が用いられている。暗号化の方式には、共通鍵方式と公開鍵方式があり、両者の利点を用いたハイブリッド方式が使用されている。共通鍵方式は処理が高速であるが、暗号鍵と復号鍵が同じため鍵が安全に送れない。一方、公開鍵方式は暗号鍵と復号鍵が異なるため、復号鍵は送付しなくてもよいが、共通鍵方式より処理速度が遅い。そのため、公開鍵方式を使用して、共通鍵方式の鍵を送付し、情報本体は共通鍵方式で暗号化して送信されている。

現在使用している公開鍵方式は、1978 年に R. L. Rivest, A. Shamir, L. M. Adelman の 3 名により発見され、RSA 暗号と呼ばれている。これは多数桁の因数分解が非常に困難なことを利用している。RSA 暗号は二つの大きな素数 P,Q 及び e をランダムに作成し、n=P×Q、F=(P-1)×(Q-1)を計算し、D=e-1 (mod F)を求め、n と e を暗号鍵として使用し、n と D を復号鍵に使用する。n と e は秘密にする必要はなく、公開鍵として自由に送信できる。一方、D は復号するための秘密鍵で、この鍵は送信しない。送付したい情報を n 以下の数値の列に分けて、それぞれを暗号化して送信し、受け取り側で復号して元に戻す。分けられて n 以下の数値を m とし、暗号文 C を C=me (mod n)で変換し送付する。受信は暗号文 C を m=CD (mod n)の変換で元の数値 m に復元する。復号は二つの素数に P,Q にオイラーの定理、M(P-1)(Q-1)=1 (mod n)を適用することで得られる。現在 n は 1024 ビット(10 進 309 桁)以上の値が使用され、P,Q はビット数が少しだけ異なるランダムな素数が使用される。

3. RSA 暗号の解読方法

RSA 暗号を解読するには、合成数 n を二つの素数 P と Q に因数分解する必要がある。現在、効率的に因数分解する方法としてふるい法が知られている。10 進 100 桁までは複数 2 次多項式ふる

い法(MPQS)が、それ以上は一般数体ふるい法(GNFS)が効率的と言われている。2 方法により合成数 n を分解する計算手順を下記に示す。

(1) MPQS(複数 2 次多項式ふるい法)

(a) ふるい処理(素数基底の選定、分解関数作成、ふるいデータ採取と行列作成)

(b) 標数 2 の線形方程式の解の計算

(c) $a^2-b^2=0 \pmod n$を構成し、n を因数分解

(2) GNFS(一般数体ふるい法)

(a) 利用する多項式(f(x))の探査

(b) ふるい処理(素数及び素イデアル基底の選定、ふるいデータ採取と行列作成)

(c) 標数 2 の線形方程式の解の計算

(d) 多項式(f(x))を法とする代数平方根の計算

(e) $a^2-b^2=0 \pmod n$を構成し、n を因数分解

RSA 暗号解読における計算量の例を表 1 に示す。これは GNFS で RSA-768(10 進 232 桁)を解読した例で、標数 2 の線形計算の次元数は 192,796,550×192,795,550 である。

表 1. RSA-768(10 進 232 桁)の計算量

処理項目	計算量(台数・年)	構成比率(%)
利用関数の探査	20	1
ふるい処理	1500	90
標数 2 の線形計算	155	9
代数平方根の計算	1	0
その他	1	0

注)計算量は ADM64(2.2Gh)の 1 コアで 1 年の計算が 1 台数・年

4. 代数的数の平方根の計算

GNFS で RSA 暗号を解読するためには代数的数の平方根の計算が必要である。計算時間は、ふるい処理や標数 2 の線形計算に比較して少ない。一般的に代数的数の平方根の計算は、中国剰余定理を上手に応用して求めている。しかし、この方法では偶数次数の場合に、分岐ケースが多岐にわたり、確実に代数的数の平方根を求めるのが困難である。ここでは、多数桁の代数方程式に変形して、その整数係数解が代数的数の平方根となる方法を使用する。この方法の利点は、計算方法が単純であり、見通しよく代数的数の平方根が求められることである。一方欠点は、数百億桁の整数係数の代数方程式の計算が必要なことである。n を因数分解する合成数とするとき、5 次式の例では下記の整数係数の方程式

$$f(\theta)=A\theta^5+B\theta^4+C\theta^3+D\theta^2+E\theta+F,\quad f(M)\equiv 0 \pmod n$$

$$H(\theta)=a\theta^4+b\theta^3+c\theta^2+d\theta+e,\quad B(\theta)=x_1\theta^4+x_2\theta^3+x_3\theta^2+x_4\theta+x_5$$

に対して

$$A^4\cdot B(\theta)^2\equiv H(\theta)\equiv(a_1\theta+b_1)(a_2\theta+b_2)\cdots(a_m\theta+b_m)\pmod{f(\theta)}$$

が成立する、整数 $x=(x_1,x_2,x_3,x_4,x_5)^T$ を求める。これは $g(x)=0$ にニュートン法を使用して、

下記の式を反復計算して求めることに帰着する。分解対象数 n が 200 桁程度の時、$H(\theta)$ を作成する一次式の項数 m は数千万で、各整数係数の値は百億桁程度になる。また、$f(\theta)$ の次数は、n が 150 桁で 5 次式、200 桁で 6 次式、250 桁で 7 次式が良いと言われている。

$$J(x^{(k)})\Delta x = g(x) = (g_1(x), g_2(x), g_3(x), g_4(x), g_5(x))^T$$

$$x^{(k+1)} = x^{(k)} - \Delta x$$

$g(x), J(x)$ を下記に示す。

$$\begin{aligned} g_1(x) = {} & (A^2C^2 - 3AB^2C + 2A^2BD - A^3E + B^4)x_1^2 + \\ & 2(A^2BC - A^3D + A^2BC - AB^3)x_1x_2 + 2A^2(B^2 - AC)x_1x_3 \\ & - 2A^3Bx_1x_4 + A^2(B^2 - AC)x_2^2 - 2A^3Bx_2x_3 + 2A^4x_2x_4 + A^4x_3^2 - a \end{aligned}$$

$$\begin{aligned} g_2(x) = {} & (A^2BE - 2ABC^2 + 2A^2C^2 - AB^2D - A^3F + B^3C)x_1^2 + \\ & 2(A^2BD - AB^2C + A^2C^2 - A^3E)x_1x_2 + 2(A^2BC - A^3D)x_1x_3 \\ & - 2A^3Cx_1x_4 + (A^2BC - A^3D)x_2^2 - 2A^3Cx_2x_4 + 2A^4(x_2x_4 + x_3x_4) - b \end{aligned}$$

$$\begin{aligned} g_3(x) = {} & (A^2BF - 2ABCD + A^2CE - AB^2E + A^2D^2 + B^3D)x_1^2 + \\ & 2(A^2BE - AB^2D - A^3F + A^2CD)x_1x_2 + 2(A^2BD - A^3E)x_1x_3 + \\ & - 2A^3Dx_1x_4 + (A^2BD - A^3E)x_2^2 - A^3Dx_2x_3 + 2A^4x_3x_5 + A^4x_4^2 - c \end{aligned}$$

$$\begin{aligned} g_4(x) = {} & (A^2CF - AB^2F - 2ABCE + A^2DE + B^3E)x_1^2 + \\ & 2(A^2BF - AB^2E + A^2CE)x_1x_2 + 2(A^2BE - A^3F)x_1x_3 - 2A^3Ex_1x_4 + \\ & (A^2BE - A^3F)x_2^2 - 2A^3Ex_2x_3 + 2A^4x_4x_5 - d \end{aligned}$$

$$\begin{aligned} g_5(x) = {} & (A^2DF - 2ABCF + B^3F)x_1^2 + 2A^2CFx_1x_2 + 2A^2BF\,x_1x_3 \\ & - 2A^3Fx_1x_4 + A^2BFx_2^2 - 2A^3Fx_2x_3 + A^4x_5^2 - e \end{aligned}$$

$$J(x) = \begin{pmatrix} \partial g_1/\partial x_1 & \partial g_1/\partial x_2 & \partial g_1/\partial x_3 & \partial g_1/\partial x_4 & \partial g_1/\partial x_5 \\ \partial g_2/\partial x_1 & \partial g_2/\partial x_2 & \partial g_2/\partial x_3 & \partial g_2/\partial x_4 & \partial g_2/\partial x_5 \\ \partial g_3/\partial x_1 & \partial g_3/\partial x_2 & \partial g_3/\partial x_3 & \partial g_3/\partial x_4 & \partial g_3/\partial x_5 \\ \partial g_4/\partial x_1 & \partial g_4/\partial x_2 & \partial g_4/\partial x_3 & \partial g_4/\partial x_4 & \partial g_4/\partial x_5 \\ \partial g_5/\partial x_1 & \partial g_5/\partial x_2 & \partial g_5/\partial x_3 & \partial g_5/\partial x_4 & \partial g_5/\partial x_5 \end{pmatrix}$$

$$= 2\begin{pmatrix} p_1 & q_1 & (A^2B^2 - A^3C)x_1 - A^3Bx_2 + A^4x_3 & -A^3Bx_1 + A^4x_2 & 0 \\ p_2 & q_2 & (A^2BC - A^3D)x_1 - A^3Cx_2 + A^4x_4 & -A^3Cx_1 + A^4x_3 & A^4x_2 \\ p_3 & q_3 & (A^2BD - A^3E)x_1 - A^3Dx_2 + A^4x_5 & -A^3Dx_1 + A^4x_4 & A^4x_3 \\ p_4 & q_4 & (A^2BE - A^3F)x_1 - A^3Ex_2 & -A^3Ex_1 + A^4x_5 & A^4x_4 \\ p_5 & q_5 & A^2BFx_1 - A^3Fx_2 & -A^3Fx_1 & A^4x_5 \end{pmatrix}$$

ここで、p_1～p_5及びq_1～q_5は下記に示す。

$$p_1 = (A^2C^2 - 3AB^2C + 2A^2BD - A^3E + B^4)x_1 + (A^2BC - AB^3 + A^2BC - A^3D)x_2 + A^2(B^2 - AC)x_3 - A^3Bx_4$$

$$p_2 = (A^2BE - 2ABC^2 + 2A^2CD - AB^2D - A^3F + B^3C)x_1 + (A^2BD - AB^2C + A^2C^2 - A^3E)x_2 + (A^2BC - A^3D)x_3 - A^3Cx_4$$

$$p_3 = (A^2BF - 2ABCD + A^2CE - AB^2E + A^2D^2 + B^3D)x_1 + (A^2BE - AB^2D + A^2CD - A^3F)x_2 + (A^2BD - A^3E)x_3 - A^3Dx_4$$

$$p_4 = (A^2CF - 2ABCE - AB^2F + A^2DE + B^3E)x_1 + (A^2BF - AB^2E + A^2CE)x_2 + (A^2BE - A^3F)x_3 - A^3Ex_4$$

$$p_5 = (A^2DF - 2ABCF + B^3F)x_1 + A^2CFx_2 + A^2BFx_3 - A^3Fx_4$$

$$q_1 = (A^2BC - AB^3 - A^3D + A^2BC)x_1 + A^2(B^2 - AC)x_2 - A^3Bx_3 + A^4x_4$$

$$q_2 = (A^2BD - AB^2C - A^3E + A^2C^2)x_1 + A^2(BC - AD)x_2 - A^3Cx_3 + A^4x_4$$

$$q_3 = (A^2BE - AB^2D - A^3F + A^2CD)x_1 + (A^2BD - A^3E)x_2 - A^3Dx_3$$

$$q_4 = (A^2BF - AB^2E + A^2CE)x_1 + (A^2BE - A^3F)x_2 - A^3Ex_3$$

$$q_5 = A^2CFx_1 + A^2BFx_2 - A^3Fx_3$$

5. 結果

ベクトル計算計算機での工夫点や結果については、講演で発表する。

6. 参考文献

[1] 木田 祐司, “数体ふるい法による素因数分解”,2003 年,
http://www.rkmath.rikkyo.ac.jp/~kida/nfs_intro.pdf