中国剰余定理　解説

最終更新日　2003 年 12 月 9 日
RSA セキュリティ株式会社　技術統括本部長　前田　司

これは、セキュリティ・ニュース（Vol.78,79）に
掲載されたセキュリティ・トピックをまとめたものです。

2004 年の RSA　Conference のテーマは、古代中国の数学・暗号技術です。
これをモチーフに展示や発表が彩られます。テーマ紹介の文章の中で古代中国数学技術力の高さを示す象徴として紹介されている Chinese　Remainder　Theorem（CRT：中国剰余定理）は、実用性と美しさを兼ね備えた「数学の宝石」の一つとも言われている整数に関する定理です。

RSA 暗号を初めとする数々の暗号技術においても、そのアルゴリズム自体の証明や実際の演算処理の高速化に利用されています。以下簡単にその内容と利用例をご紹介します。

まず、この定理がカンファレンスのテーマとして採用された“中国”を名前にいただく所以ですが、紀元３世紀頃中国において、官僚の教育用教科書として用いられた「孫子算経」という数学書にその定理の具体例が、数学の難問として掲載され、それが世代を超えて伝承され 13 世紀に秦九韶によりその著書「数書九章」の中で定理として整理されたことによります。18 世紀にヨーロッパにその内容が紹介され、ガウスの解法と一致することが判明するにいたり、世界的に中国数学技術の成果として認識されました。
「孫子算経」は古代日本にも紹介され、古代律令制を支えた役人の教育用に利用されました。養老令に記述があります。

さて、その「孫子算経」にある具体例ですが、「物不知数」問題と称され、次のようななぞなぞとして紹介されています。

「今有物不知其数、三三数之剰二、五五数之剰三、七七数之剰二、問物幾何。」

意訳すると、3で割れば（3を次々と引くと）2余り、5 で割れば3あまり、7 で割れば2あまる数はなあんだ？となります。回答は

「術曰、三三数之剰二置一百四十、五五数之剰三置六十三、七七数之剰二置三十、併之、得二百三十三、以二百一十減之、即得。」

3 で割った(3を次々と引いた)余り2を140とし、5 で割った余り3を63とし、7 で割った余り2を30とし、それらを合わせて233、それから210を引いて求まる。
と書かれています。

さらに、この問題を一般化した公式として、

「凡三三数之剰一則置七十、五五数之剰一則置二十一、七七数之剰一則置十五。一百六以上、以一百五減之、即得。」

3 で割った余りに70をかけ、5 で割った余りに21をかけ、7 で割った余りに15
をかけ105を引いていって106より小さくなった余りが答え
が紹介されています。

この公式が次のような民謡(孫子歌と呼ばれ、色々な種類があるようです)として伝えられています。
古代の役人が苦労して公式を暗記した様子がしのばれます。

三人同行七十里

五樹梅花廿一枝

七子團圓正月半

一百零五轉回起

この問題は、その問題の冒頭の「この数なあんだ」という部分から「物不知数」あるいは最後に105を引いてゆくことから「百五減算」問題と呼ばれ後世に伝えられてきました。後にその理論が解明されるまで、古代からの不思議な問題としてその公式だけが伝わり利用されてきたようです。

さて、この「百五減算」問題を現代の数学記号を使って記述すると次のようになります。

X≡2 (mod 3)
X≡3 (mod 5)
X≡2 (mod 7)

を同時に満たす整数 x を求めよ。
ここで X≡a (mod m)は x－a が m の倍数となることを表し、m を法として合同であるといいます。これはつまり m で割った余りが同じだということです。上の例では a が m より小さいので、x を m で割った余りが a であると考えてかまいません。

一見、3 で割って 2 余る数なんて無限に有るし、5 で割って．．．．．、こんな答えは無限に有るようにも思えますし、逆にこんなうまい数字があるようには思えない感じもするのですが、もちろん答えは上に述べたように存在し、しかも、それはたった一つです（だからこそ「百五減算」問題などといって不思議がられたのですね）。

この少し不思議な問題が、次のように拡張一般化されやがて中国剰余定理と呼ばれるようになりました。

中国剰余定理

正の整数 $n_1, n_2, \ldots, n_k$ が、2 つずつ互いに素（最大公約数が 1）であるとき、任意の整数 $a_1, a_2, \ldots, a_k$ に対し、連立合同式、

$x \equiv a_1 \pmod{n_1}$
$x \equiv a_2 \pmod{n_2}$
……
$x \equiv a_k \pmod{n_k}$

には、解 x が存在し、その解はすべて $N=n_1n_2\ldots n_k$ を法として合同である。

「百五減算」問題では 105 が N にあたることがお分かりだと思います。105 で割った余りが問題の解答ですから、「百五減算」問題の解はただ一つです。

この定理を示し、その解法を著したのが先に述べた秦九韶というわけです。秦九韶は「百五減算」の解法を、
bx≡1 (mod c)
という形の剰余方程式の解法に結び付けました。これは現在 Gauss の方法として知られている大変美しい解法と同じ内容です。秦九韶はユークリッドの互除法を使ってこの方程式を解く解法を示しています。この一連の解法は「大衍求一法」と名づけられ、秦九韶の重要な成果と考えられています。

この mod の算術体系を最初に「体系的」・「論理的」に整備したのは Gauss です。19 世紀初めのことです。13 世紀中国に mod のような記号はありませんし、記述はすべて漢字でおこなわれています。しかも算木の使用を前提とした解法なので大変アルゴリズム的な記述です（算盤を習われたことがある方なら例えば $\sqrt{\ }$ の求め方をどのように習ったかを思い出されるでしょう）。

現代を生きる我々には、数学といえば、秦九韶の算法的数学よりも Gauss の弁証法的数学の方がなじみやすいと思います。しかも Gauss の剰余式に関する体系が無ければ今の暗号技術はもちろん有りません。しかし、暗号実装の最大の舞台であるコンピュータがアルゴリズム（算法）表現の権化であることを思うと、算木による実学的な算法的数学として生まれた剰余の世界が抽象的な演算体系としてまとめられ、やがて算法的実装として再び開花するという流れに大きな歴史のリズムのようなものが感じられます。

さて、以上のように古い歴史を持つ中国剰余定理ですが、今ひとつその意味するところがピンと来ない方もいらっしゃるのではないかと思います。なぞなぞの答えの存在を保証する定理が何故それほど重要なのかと。

そこで代表的暗号手法である RSA 暗号に中国剰余定理がどのように関わっているのか、2つ程例をあげてご紹介したいと思います。

# # #

中国剰余定理は連立合同式の式の数に制限はありません。典型的な RSA 暗号に応用するためには 2 つの式で十分です。例えば百五減算問題の最初の 2 式を使いましょう。

$X \equiv 2 \pmod 3$
$X \equiv 3 \pmod 5$

これを満たす数を見つけます。
簡単な計算で X=8 であることがわかります。正確には $X \equiv 8 \pmod{15}$ となる X ですね。

一般的に書きますと

$x \equiv a_1 \pmod{n_1}$ （1）
$x \equiv a_2 \pmod{n_2}$ （2）

を満たす解が必ず唯一存在しそれは

$x \equiv a_3 \pmod{n_1 n_2}$ （3）

を満たすと、なります。

これは、n_1n_2 を法とする合同式が n_1 と n_2 それぞれを法とする 2 つの合同式に対応付けられるということを示しています。中国剰余定理を使うと、ある数 n を互いに素である2つの数の積に分解できる時、n を法とする合同問題はより小さな 2 つの合同式の計算に還元できるというわけです。上の例ですと、

15 を法とする合同式　　3 と 5 それぞれを法とする 2 つの合同式

8　　⇔　　2 と 3

さてここで、RSA 暗号の基本式を復習しておきます。

大きな2つの素数 p と q を用意し、

n=p･q

e を(p－1)･(q－1)と互いに素である正の整数

d を e･d≡1 mod ((p－1)･(q－1))を満足する正の整数とする。

暗号化するメッセージを M、暗号文を C とすると、

RSA 暗号化（あるいは署名検証）　$C \equiv M^e \pmod n$

RSA 復号化（あるいは署名生成）　$M \equiv C^d \pmod n$

e と n が公開鍵、d（と n）が秘密鍵です。

n は大変大きな数字で最近では 2^{1024} のオーダーの数が一般的です。

ＲＳＡ暗号は、べき乗剰余演算だけで構成される大変シンプルな暗号方式で、初めてその式を目にする方はそのシンプルさと対称性の美しさに驚かれます。暗号化･復号化両方ともに同じべき乗剰余演算を行うことがＲＳＡ暗号方式の大きな特徴ですが、その表現のシンプルさとは裏腹に、コンピュータ上で大きな数を法とするべき乗演算は大変な計算量を必要とします。

暗号化に使われる公開鍵 e は一般に小さな値なので、まじめに計算してもそれほど時間はかかりませんが、復号化のための秘密鍵 d は大きな数字となりますので、実装においては高速に処理をおこなうためのさまざまな工夫が凝らされます。そのもっとも有効なものの一つが中国剰余定理を用いた高速化です。

n は p と q（素数同士ですからもちろん互いに素です）の積ですから、中国剰余定理が主張するように、復号化の式を p と q を法としたより小さな合同式に分けることができます。一般に n を法とするべ

き乗の計算量は n の長さの3乗に比例するといわれています。p と q はほぼ同じ長さにすることが普通ですから、n のまま計算すると n^3 の計算量を要すところ、p と q に分けると $(n/2)^3+(n/2)^3=n^3/4$ の計算量で済みます。中国剰余定理を応用すると計算量は 1/4（＋中国剰余定理を解くための演算時間）になるわけです。

中国剰余定理を利用するためには p と q を知らなくてはいけませんから、この高速化を、公開鍵を利用して暗号化（あるいは署名検証）する側の人に利用させるわけにはいきませんが（n が因数分解できれば秘密鍵がばれてしまいます）、上に述べたように暗号化演算はあまり計算量を要しないので中国剰余定理を用いなくても問題なく、中国剰余定理を利用するのはもっぱら復号化演算（秘密鍵演算）です。そのため秘密鍵の保存の際、n も p と q に分けられたまま（秘密に）保管されます。

中国剰余定理を説くためには Gauss の方法があると上述しましたが、n が大きい場合にはコンピュータ内での演算を考慮したより有効な（高速）解法が存在します。Gauss の方法の美しさもコンピュータの愚直な繰り返し演算には用無しというわけです。

さて、上で述べた RSA 暗号は n が3つ以上の素数から構成されていても成立します。
中国剰余定理は連立合同式の数に制限は無いことは先に述べました。また、法の数の長さが短くなればなるほど計算量が少なくなるわけですから、n をできるだけ細かな素数の積に分解したほうが、より高速の復号化処理が可能となります。また RSA 暗号を解読するためには n を因数分解することが一般的ですが、現在知られているもっとも効率の良い因数分解の方法(数体ふるい法)は n の長さに計算量が依存します。ですから n の長さを変えずに n を構成する素数を増やしていった方がより計算の効率があがるように思えます。
しかし残念なことに因数分解の方法には、構成する素数の長さに計算量が依存する手法(例えば楕円曲線法)も存在し、素数を増やしてそれぞれの長さを短くしていくと、やがて、そちらの手法の方が効率良く因数分解できるようになります。そのため、n の長さに応じて増やせる素数の数には制限があります。
現在一般的である n の長さ 1024 ビット（から 3500 ビットぐらいまで）では素数の数3個が暗号強度を損ねない限界です。素数の数を3個にすることにより中国剰余定理を利用しない場合に比べ必要計算量は 1/9 になる計算です。この、素数の数を増やす方法は MultiPrime と呼ばれ Hewlett-Packard 社が特許を持っています。秦九韶が知ったらさぞ驚くことでしょう（宣伝になりますが MultiPrime は RSA セキュリティがライセンスしており、暗号ツールキット製品 RSA BSAFE で利用可能です。ご利用ください）。

さて、RSA 暗号と中国剰余定理の関わりをもう一つご紹介します。

実はＲＳＡ暗号の解読の困難性の根拠それ自体に中国剰余定理が顔を見せます。話は少し込み入

りますがお付き合いください。

復号化の式の証明をダイレクトに書くと次のような流れになります。

$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M \pmod n$ ？

「ああ、$e \cdot d \equiv 1 \bmod ((p-1)\cdot(q-1))$だから」とおっしゃる方は、早とちりか、RSA の発明者 Rivest 先生並に鋭い方かどちらかです。mod ((p－1)・(q－1))と(mod n)とで、法となる数が違っています。

ここでちょっと寄り道です。Euler（オイラー）の定理と呼ばれる美しい式があります。
ある整数 M と正の整数 n が互いに素な時、
$M^{\Phi(n)} \equiv 1 \pmod n$
が成り立つというものです(証明については数論の教科書あるいは Web でご確認ください)。
$\Phi(n)$はオイラー関数と呼ばれています。0 と n の間で n と互いに素な整数の個数を表わします。

例えば、10 までの整数のオイラー関数は次の通りです。

n	1	2	3	4	5	6	7	8	9	10
$\Phi(n)$	1	1	2	2	4	2	6	4	6	4

n が素数の場合に$\Phi(n) = n-1$ となるのはご理解いただけると思います。
またオイラーはオイラー関数に関しもう一つ公式を残しています。p と q が互いに素の時、
$\Phi(p\cdot q) = \Phi(p)\cdot\Phi(q)$
が成り立つというもので、オイラーの積公式と呼ばれています。

さて話を RSA の式に戻します。オイラーの積公式を使うと、p と q が素数ですから、
$e\cdot d \equiv 1 \bmod ((p-1)\cdot(q-1)) \rightarrow e\cdot d \equiv 1 \bmod (\Phi(p)\cdot\Phi(q))$
$\rightarrow e\cdot d \equiv 1 \bmod (\Phi(p\cdot q)) \rightarrow e\cdot d \equiv 1 \bmod (\Phi(n))$
つまり $e\cdot d$ は$\Phi(n)$の整数倍+1 ということです。そこで $e\cdot d = k\cdot\Phi(n)+1$ とおくと、
$M^{ed} \equiv M^{k\cdot\Phi(n)+1} \bmod(n)$ (k は整数)
がなりたちます。M と n が互いに素の場合にはオイラーの定理より
$M^{ed} \equiv M^{k\cdot\Phi(n)+1} \equiv (M^{\Phi(n)})^k \cdot M \equiv M \bmod(n)$
として証明が完了します。
実際は $n = p\cdot q$ ですから、M が p あるいは q で割り切れる（オイラーの定理の前提である互いに素という条件が成り立たない）場合をきちんと始末しなくてはすべてのメッセージ M に通用する暗号にはなりませんが、この場合にも上式が成り立つことが証明できます（RSA 暗号に関するオリジナルの論文をご参照ください）。

さて、オイラーの公式だけで RSA **暗号の証明が終了してしまいました。**
中国剰余定理が出る幕が無いように見えるのですが、実はオイラーの積公式は、ある条件のもとで中国剰余定理がもたらす整数集合の性質を表わしています。簡単に述べますと中国剰余定理

$x \equiv a_1 \pmod{n_1}$
$x \equiv a_2 \pmod{n_2}$

を満たす解が必ず唯一存在しそれは
$x \equiv a_3 \pmod{n_1 n_2}$
は、a_1 **と** n_1、a_2 **と** n_2、a_3 **と** $n_1 n_2$ **がそれぞれ互いに素である場合に限っても成り立ちます。**

先に述べた一般的な中国剰余定理は任意の整数の組 a_1、a_2 **で成り立ちますが、それが** a_1 **と** n_1、a_2 **と** n_2 **がそれぞれ互いに素である場合に限定しても成り立ち、その解** a_3 **も** $n_1 n_2$ **と互いに素になります（またその逆）。その時** a_1、a_2、a_3 **がとり得る値の個数がφになっています。オイラーの積公式は** a_1 **と** a_2 **の組み合わせの数だけ** a_3 **があることを示しているわけです。先の例で言いますと、**

15 **を法とする合同式**	⇔	3 **と** 5 **それぞれを法とする** 2 **つの合同式**
15 **と互いに素な** a_3	⇔	3 **と互いに素な** a_1 **、**5 **と互いに素な** a_2
{1, 2, 4, 7, 8, 11, 13, 14}	⇔	{1, 2}**と**{1, 2, 3, 4}

の対応が中国剰余定理から保証され、

1	⇔	1 **と** 1
2	⇔	2 **と** 2
4	⇔	1 **と** 4
7	⇔	1 **と** 2
8	⇔	2 **と** 3
11	⇔	2 **と** 1
13	⇔	1 **と** 3
14	⇔	2 **と** 4

となります。これより

$\phi(15) = \phi(3) \cdot \phi(5) = (3-1) \cdot (5-1) = 2 \cdot 4 = 8$

がわかります（3 **と** 5 **は素数です）。**

RSA **は素因数分解の困難性を根拠にした暗号ですが、これは** RSA **暗号文を解読するためには、秘密鍵** d **を求めることが知られているもっとも有効な方法であるという認識のためです。**d **を求めるためには** n **よりφ(**n**)つまり(**p**−**1**)・(**q**−**1**)を求めなくてはいけません。逆に、もし何らかの(他の)方法で** d

が計算できるのであればその d をもとに n の素因数分解を効率よく行う方法が存在します。

素数 p と q より導出された e と d が中国剰余定理（オイラーの積公式）により p・q＝n を法とする復号化の式の中へ組み込まれる様子を見ると、中国剰余定理が RSA 秘密鍵と公開鍵の関係を裏付けていると言って良いのではないかと思います。RSA 暗号の困難性の根拠となる素因数分解は中国剰余定理での対応付けをさぐる行為でもあるわけです。百五減算が不思議がられるのは当然のことです。

（完）