ＲＳＡ暗号と素因数分解

林　　雄一郎*

1　はじめに

今日、インターネット上の商取引や重要文書の通信セキュリテイ、デジタル・ファイルの管理に暗号化ソフトが使われている。これにはRSA暗号方式が使われている。これは、1977年MITのRivest、Shamir、Adlemanのグループが考案したもので彼らの頭文字をとってRSA暗号としている。彼らはこの功績でTuring賞（2002年）を受賞した。この暗号には初等整数論のいろいろな性質や巨大素数からなる巨大合成数が活用されている。もしこの数が意図的に因数分解できればたちまち暗号は解読されセキュリテイは破綻する。本稿では、この暗号体系にかかわる整数論や素因数分解問題の話題を提供する。

2　RSA暗号

通信文を数値化して通信aとする。また、大きな2つの素数p,qを選び（素数か否か判定が必要）その積Nを定めておく。また、$(p-1)(q-1)$（Euler関数$\varphi(N)$）と互いに素なある整数r（閉める鍵）を選ぶ。このとき$a^r \equiv b \pmod N$　となるbが暗号となる。N,rは公開される（公開鍵暗号）。受信側は、暗号bから元の通信aを復元するには次のような手順が必要となる。

まず、公開鍵Nを素因数分解し、p,qを知る。一般に、大きな整数の素因数分解は適切な時間（例えば多項式時間）、記憶容量内で処理するのは困難な問題である。これがRSA暗号の安全性を確保している。復元は、$rs \equiv 1 \pmod N$　となるs（開ける鍵）を、p,q,rを用いて求め、暗号bをs乗し、法Nに関する剰余を求める。$b^s \equiv (a^r)^s = a^{rs} \equiv a^1 = a \pmod N$　となる。

3　準備

RSA暗号に用いられる初等整数論の知識を簡単にまとめておく。

（1）不定方程式が解をもつ条件

不定方程式　$ax+by=c$　が解をもつためには、$gcd(a,b)|c$　が必要十分条件である。

（証）必要条件は明らかである。十分条件は、$n=Min\{ax+by|ax+by>0\}$とおくと、$ax+by=m$となる数mはnの倍数になる。何故なら、$m=nq+r$　$0\le r<n$　$as+bt=n$　$ax+by=m$

$r=m-nq=(ax+by)-(as+bt)q=a(x-sq)+b(y-tq)$　nの最小性から$r=0$となる。

$a=a\cdot1+b\cdot0$　$b=a\cdot0+b\cdot1$　よって、a,bはnの倍数。つまり、nはa,bの公約数であるから、

＊北海道情報大学情報メディア学科

$d=gcd(a,b)$の約数。　$n \le d$　他方、nはa,bの１次結合$as+bt$と表されているから、dの倍数となり$d \le n$　よって　$n=d$　したがって、$d=as+bt$　でありdの倍数cもa,bの１次結合で表される。

（２）Eulerの定理、Fermatの定理

Eulerの関数$\varphi(N)$は、１からNまでの自然数でNと互いに素な数の個数を表す。

pが素数ならば$\varphi(p)=p-1$　qも素数で$N=pq$ならば　$\varphi(N)=(p-1)(q-1)$

（証）1から$(N-1)$までの数でp,qの倍数はそれぞれ$(q-1),(p-1)$個ずつあるから

$$\varphi(N)=pq-1-(p-1)-(q-1)=pq-p-q+1=(p-1)(q-1)$$

（Eulerの定理）　自然数m、整数aに対して$gcd(a,m)=1$ならば$a^{\varphi(m)} \equiv 1 (mod\ m)$

（証）　$\{x_1,x_2,\cdots,x_l\}$を 法mに関する既約剰余系とする。$l=\varphi(m)$　このとき、ax_iはmと互いに素だから$\{ax_1,ax_2,\cdots,ax_l\}$はまた既約剰余系となる。$(ax_1)(ax_2)\cdots(ax_l) \equiv x_1x_2\cdots x_l (mod\ m)$

$$a^l x_1x_2\cdots x_l \equiv x_1x_2\cdots x_l (mod\ m) \qquad (x_1x_2\cdots x_l, m)=1 \qquad a^l=a^{\varphi(m)} \equiv 1 (mod\ m)$$

Eulerの定理で$N=p$（素数）とすれば$\varphi(p)=p-1$　$gcd(a,p)=1$のとき、$a^{p-1} \equiv 1 (mod\ p)$

これはFermatの小定理である。なお、$x \equiv 1 (mod\ p-1)$　ならば　$a^x \equiv a (\mathrm{mod}\ p)$　が成り立つ。　（証）$x=1+(p-1)A$　とおけば　$a^x=a^{(p-1)A+1}=\left(a^{p-1}\right)^A \cdot a \equiv 1^A \cdot a=a(mod\ p)$

4　s,aを求める計算

$gcd\,(r,p-1)=1, gcd\,(r,q-1)=1$　だから次の１次不定方程式は解をもつ。

$ur+v(p-1)=1$　　$xr+y(q-1)=1$　２式から　$(u-x)r=-v(p-1)+y(q-1)$

$gcd(p-1,q-1)=d$とすれば、　$d \mid (u-x)$　となる。よって、次の不定方程式は解を持つ。

$w(p-1)+(q-1)t=u-x$　この不定解の一組をw, t とし、$u-w(p-1)=x+t(q-1)=s$とおくと、このsが求めるものである。

$$rs = r\big(u - w(p-1)\big) = ru - rw(p-1) = 1 - v(p-1) - rw(p-1) \equiv 1 \pmod{p-1}$$

$$rs = r\big(x + t(q-1)\big) = rx + rt(q-1) = 1 - y(q-1) + rt(q-1) \equiv 1 \pmod{q-1}$$

よって、$rs \equiv 1 \pmod{p-1}$　　$rs \equiv 1 \pmod{q-1}$　から$a^{rs} \equiv a \pmod{p}$　　$a^{rs} \equiv a \pmod{q}$

したがって、$a^{rs} \equiv a \pmod{pq} = a \pmod{N}$　となり復元される[1]。

なお、r,sは有限体Z/pZにおいて乗法に関して互いに逆元である。

例　$p = 11, q = 13, n = pq = 143, r = 7, a = 5$とする。平文は5、暗号文は$47 \pmod{143}$である。

$a^7 = 5^7 = 78125 = 546 \times 143 + 47 \equiv 47 \pmod{143}$　解読を考える。次の不定方程式の特殊解を求める。

$7u + 10v = 1, 7x + 12y = 1$　拡張されたEuclidの互除法を用いて

$10 = 1 \times 7 + 3, 7 = 2 \times 3 + 1$から$1 = 7 - 2 \times (10 - 1 \times 7) = 3 \times 7 - 2 \times 10$　$u = 3, v = -2$

$12 = 1 \times 7 + 5, 7 = 1 \times 5 + 2, 5 = 2 \times 2 + 1$から

$1 = 5 - 2 \times (7 - 1 \times 5) = 3 \times 5 - 2 \times 7 = 3 \times (12 - 1 \times 7) - 2 \times 7 = 3 \times 12 - 5 \times 7$　$x = -5, y = 3$

$u - x = 8$より、不定方程式　$8 = 10w + 12t, 4 = 5w + 6t$　の特殊解は　$w = -4, t = 4$

そこで　$s = u - w \times 10 = x + t \times 12 = 3 + 4 \times 10 = -5 + 4 \times 12 = 43$　$47^{43} \pmod{143}$が解読した結果（10進72桁の数）となる。なお、Mathematicaで　Mod[47^43,143]の結果は5となる。

5　素数の判定

数nに対して、良く知られた$\sqrt{n}$以下のすべての素数で試すEratosthenesの篩法は、$\sqrt{n}$以下のすべての素数での割り算を試すので効率が悪い。一般に、$1 \le k \le n$、$gcd(k,n)$を求める計算回数はkの10進桁数の5倍以下となる（*Lamė*の定理）。例えば$n = 10^{50}$ $m = \left[\sqrt{n}\right]$とすると計算総数は高々$5\sum_{k=1}^{m} log_{10} k = 5log_{10} m! \approx 5log_{10}\left(\sqrt{2\pi}\left(m^{m+1/2}\right)e^{-m}\right)$（Stirlingの公式）これに$m = 10^{25}$を代入し計算すると$1.27172 \times 10^{27}$、1回の互除法の平均計算が100億分の1秒としても40億年かかる。

次に、Fermatの小定理の対偶を用いた方法（Fermat-test）がある。ランダムに選んだ$a(1 \le a \le n-1, gcd(a,n) = 1)$について、$a^{n-1} \equiv 1 (\mathrm{mod}\, n)$が成り立つかどうか調べ、成りたたなければ$n$が合成数となる。

また、直接、素数判定する優れたアルゴリズムMiller-Rabin法がある。nは奇数とする。

①nに対して、$1 \le b \le n-1$である整数b（底という）をランダムに選ぶ、②$n-1=2^s \cdot d$（dは奇数）となるs,dを求める、③$b^d \equiv 1 \pmod{n}$であるか、または、ある$r\left(0 \le r \le s-1\right)$について$b^{2^r \cdot d} \equiv -1 \pmod{n}$であるかを調べる、④上の条件を満足しない$b$が見つかれば$n$は合成数であるし、そうでなければ素数である確率は高いことになる。

nは奇素数　$gcd(b,n)=1$　$n-1=2^s \cdot d$　dは奇数とする。このとき、$(Z/nZ)^{\times}$の任意の要素bに対して、次の(a),(b)いずれかが成り立つ。(a)　$b^d \equiv 1 \pmod{n}$、(b)$b^{2^r \cdot d} \equiv -1 \pmod{n}$

（証）Fermatの定理より、$b^{n-1} \equiv 1 \pmod{n}$　$b^{n-1} = b^{2^s \cdot d} = \left(b^{2^{s-1} \cdot d}\right)^2 \equiv 1$より$b^{2^{s-1} \cdot d} \equiv 1$または$-1$である。ここで、$Z/nZ$は整域だから（$\bar{a} \cdot \bar{b} \equiv \bar{0}$ならば$\bar{a} \equiv \bar{0}$または$\bar{b} \equiv \bar{0}$）、$\bar{x}^2 \equiv \bar{1}$より$\bar{x} \equiv 1$または$\bar{x} \equiv \overline{-1} = -\bar{1}$が成り立つ。もし、$b^{2^{s-1} \cdot d} \equiv -1$なら(b)が成り立つ。また、$b^{2^{s-1} \cdot d} \equiv 1$ならば同様にして$b^{2^{s-2} \cdot d} \equiv 1$または$-1$となる。以下、同様の議論を続けると、$s-1 > s-2 > \cdots = 0$となる。

最後は、$b^{2^0 \cdot d} = b^d \equiv 1 \pmod{n}$となり、(a)が成り立つ。（証明終わり）この命題の対偶は、「ある$b \in (Z/nZ)^{\times}$が存在して、(a),(b)の両方が成り立たないならば、nは素数ではない」となる。これを確かめるのがMiller-Rabin法である。k回bを選び調べる試行で、(a)または(b)が成り立ち、nが奇素数と誤る（このbは“強い嘘つき”）確率は4^{-k}以下であることが分かっている[2]。

6　巨大数の因数分解

多項式時間のアルゴリズムとは、入力サイズnに対して、処理時間の上界がnの多項式で表現されるものである。例えば、バブルソートは　n(n—1)/2 で要素数nの2次多項式となる。

このように多項式時間（Polynomial time）で決定性アルゴリズムによって解ける問題はP問題と呼ばれる。他方、NP（Non-deterministic Polynomial time）問題は次の①、②のいずれかの条件（この2つは同値）を満たす問題の集まりである。①非決定性アルゴリズムによって多項式時間で解ける、② 確たる証拠が与えられたとき、それが正しいか否かを多項式時間で検証できる。非決定性アルゴリズムはそのプロセスにランダム性を含むものである。NP問題は$n!$、2^nなど階乗・指数時間を要する問題群である。$P \subset NP$は成立するがPが真部分集合かどうかという「$NP \neq P$予想」は未解決問題である。NPに属する問題と同じ位難しい問題はNP困難問題と呼ばれる。

巨大数の因数分解は、従前のアルゴリズムの多く（数体篩法、楕円曲線法など）は決定性アルゴリズムであるが、最も効率の良い方法でも準指数時間（多項式時間と指数時間の中間）を要するためＮＰ困難問題であり、多項式時間のアルゴリズムは今のところ求められていない。

例　$2^{19937}-1$　をmathematicaで因数分解してみると別添資料のようになる。これは6002桁のMersenne素数である。

最近、量子コンピュータが実現し、重ね合わせを用いて超並列計算が可能となっている。1994年にShorが量子コンピュータ専用の非決定性アルゴリズムを考案し発表した。

Shor アルゴリズムとその証明は次のようになる。素因数分解したい合成数をnとし、$n=pq$かつp,qは素数と仮定する。①　$\{1,2,3,\cdots,n\}$からランダムに選びaとおく、②　$\gcd(a,n)=1$なら③へ行く。そうでないなら①に行く、③$a^r\equiv 1(\mathrm{mod}\,n)$となる$r$を、量子コンピュータで求める、④$r$が偶数ならば⑤に行く。奇数ならば①に行く、⑤$\gcd\left(a^{r/2}+1,n\right),\gcd\left(a^{r/2}-1,n\right)$を求める、⑥　⑤で求めた数のいずれかが$n$ならば①に戻る。そうでなければこれらの数が求める素因数p,qとなる。

$p=\gcd\left(a^{r/2}+1,n\right),q=\gcd\left(a^{r/2}-1,n\right),a^r-1=nn',n=pp''=qq'',a^{r/2}+1=pp',a^{r/2}-1=qq'$

$\gcd(p',p'')=\gcd(q',q'')=1$　　$a^r-1=\left(a^{r/2}+1\right)\left(a^{r/2}-1\right)=pp'qq'=nn'=pp''n'=qq''n''$ これから

$p'qq'=p''n',pp'q'=q''n'$　　$p'|n',q'|n'$　から$n'=p'q'l$　　$p=q''l$　　pは素数だから$p=q'',l=1$

または$p=l,q''=1$　　$n=pq$となる。$q=p''l$からも同じ結果が出てくる。（証明終わり）

③では、複数のr値を選び、それぞれの計算を並行に走らせ（マルチタスク）成り立つものが出てくれば終了させる木構造の計算となる。また、⑤はユークリッド互除法を使う。このアルゴリズムの計算量は、数nを2進数表示したとき桁数$\log_2 n$に関する多項式時間となる[3]ことが分かっている。例えば、$n=21$にShorアルゴリズムを適用してみる。①で、$a=2$を選ぶと$(2,21)=1$だから③に行く。$2^r\equiv 1(\mathrm{mod}\,21)$となる最小の$r$は、$2^6=64=3\times 21+1$　なので6である。④に行きrは偶数だから⑤に行く。⑤では、$2^{\frac{6}{2}}+1=9,2^{\frac{6}{2}}-1=7$　$\gcd(9,21)=3,\gcd(7,21)=7$　よって、$p=3,q=7$となり因数分解出来たことになる。

7　終わりに

整数論の定理が身近なインターネットにおける通信処理に生かされていることを知れば、数学、特に整数論に対する興味・関心が増すであろうし、数学に対する価値観を改善するきっかけとなる。新数学Aの整数論の授業での話題としてみてはどうか。

参考文献（1）一松信：暗号の数理、講談社ブルーブックス、昭和55年

（2）深川久：Miller-Rabinによる素数の確率的判定法、大阪市立大学、2002

（3）栗山、佐野、古市：shorの素因数分解アルゴリズムにおける計算量の精密な評価
統計数理研究所、講究録1452巻、2005

```
{{43154247973881626480552355163379198390539350432267115051652505414033306801
376580911304513629318584665545269936257648835317902217334584413909528269
154609168019040787534374139629680180192011448648090266141431844327698030D066
728104984095451588176077132969843762134621790396391341285205627619600513
106646376648615994236675486537480201964350295935168662363909047948347692
313978301377820785712419054474332844529183172973242310888265081321626469
451077707812282829444775022680488057820028764659399164766265200900561495
800344054353690389862894061792872011120833614808447482913547328367277879
565648307846905116945866230169702401260240187028746650033445774570315431
292996025187780790119375902863171084149642473378986267503308961374905766
340905289572290D16D38000571630875191373979555047468154333253474991046248
132504516341796551470575481459200B59472614836213875557126864445789750886
277996487304308450484223420629266518556024339339190844368921018424844677
042727664601852914925277280922697538426770257333928954401205465895610347
658855386633902546289962132643282425748035786233580608154696546932563833
327670769899439774888526687278527451002963059146963875715425735534475979
734463100678367393327402149930968778296741391514599602374213629898720611
431410402147238998090962818915890645693934483330994169632295877995848993
366747014871763494805549996163051541225403465297007721146231355704081493
098663065733677191172853987095748167816256084212823380168625334586431254
034670806135273543270714478876861861983320777280644806691125713197262581
763151313596429547763576367837019349835178462144294960757190918054625114
143666384189433852576452289347652454631535740468786228945885654608562058
042468987372436921445092315377698407168198376538237748614196207041548106
379365123192817999006621766467167113471632715481795877005382694393400403
061700457691135349187874888923429349340145170571716181125795888889277495
426977149914549623916394014822985025331651511431278802009056808456506818
877266609831636883884905621822262933986548645669080672191704740408891349
835685662428063231198520436826329415290752972798343429446509992206368781
367154091702655772727391329424277529349082600585884766523150957417077831
910016168475685658673292860882407D179760307269849987354836042371734660257
694347235506301744118874141292438958141549100609752216802230887611431996
472330842380137110927449483557815037586849644585749917772869926744218369
621137675101083278543794081749094091043084096774144708436324279476892056
200427227961638669149805489831121244676399931955371484012886360748706479
568669048574782855217054740113945929622177502575565811067452201448981991
968635965361551681273982740760138899638820318776303668762730157584640042
798880691862640268612686180893874939573818125022279689930267446255773989
542469831637863000171279227151406034129902181570659650532600775823677398
182129087394449859182749999007223592423334567850671186568839186747704960
016277540628331440619019139983789914712515365200336057993808601678807687
568562377857095285841304902927192220184172502357124449911870210642694565
061384919373474324503966267799038402386781686809962015879090586549423504
699190743519551043722544515740967829084336025938225780730880273855261551
972044075620326780624448803490998232161231687794715613405793249545509528
052518010123087258778974115817048245588971438596754408081313438375502988
726739523375296641615501406091607983229239827240614783252892479716519936
989519187808681221191641747710902480633491091704827441228281186632445907
145787138351234842261380074621914004818152386666043133344875067903582838
283562688083236575482068479639546383819532174522502682372441363275765875
609119783653298312066708217149316773564340379289724393986744139891855416
612295739356668612658271234696438377122838998040159739078061443675415671
078463404673702403777653478173367084844734702056866636158138003692253382
209909466469591930161626097920508742175670306505139542860750806159835357
541032147095084278461056701367739794932024202998707731017692582046210702
212514120429322530431789616267047776115123597935404147084870985465426502
772057300900333847905334250604119503030001704002887892941404603345869926
367501355094942750552591581639980523190679610784993580896683299297681262
442314008657033421868094551740506448829039207316711307695131892296593509
018623094810587519560305240787163809219164433754514863301000915916985856
242176563624771328981678548246297376249530251360363412768366456175077031
977457534912806433176539995994343308118470147158712816149394421276614228
262909950055746981053206610001560295784656616193252269412026831159508949
671513845195883217147982748879261851417819979034417285598607727220866677
680426090308754823803345446566305619241308374452754668143015487710877728
011086004325892262259413968285283497045571062757701421761565262725153407
407625405149931989494459106414660534305378576709862520049864880961144869
258603473714363659194013962706366851389299692869491805172556818508298824
954954815796063169517658741420159798754273428026723452481263569157307213
153739781041627683715078598504184797287663122946711348158529418816432825
044466692781137474494898385064375787507376496345148625306383391555145690
087891955315994462944493235248817599907119135755933382121706191477185054
936632211157222920331148502487563303118018805685073569841580518118710778
653953571296014372940865270407021524383167290323231567912289419486240594
039074452331678019381871219092185460768444573578559513613304242206151356
457513937270939009707237827101245853837678338161023397586864894230696091
540249987907453461311923963852950754758058205625956600817743007191746812
655955021747670922460866747744520875607859062334750627098328593480067789
456169602494392813763495657599847485773563990957557313200809040830036446
492219409934096948730647494301216165686750735749555882340303989874672975
455060957736921559195480815514035915707129930057027117286252843197413312
307617886797506784260195436760305590340708481464607278955495487742140753
570621217198252192978869786916734625618430175454903864111585429500569920
905636741539030968042471。1)}
```