現代の暗号

雪江明彦

1　簡単な暗号

今日は現在使われている暗号のうち RSA 暗号というものについて話したいと思います。私の専門は整数論というものです。純粋数学としての整数論は，方程式にどれくらい整数解があるかとか，素数がどれくらいあるとか，純粋な興味を追求するもので，理論として大変美しいものですが，今日はそういう難しい理論ではなく，実社会で実際に使われているような応用について話したいと思います。この話の後半では，皆さんに RSA 暗号で作られた暗号文を，非常に簡単な場合に平文に復元するという作業をしてもらって，整数論を使った暗号を体験していただきたいと思います。

まず最初に原始的な暗号とその問題点についてお話しします。次の表を見てください。

X	Y	X	Y	X	Y	X	Y	X	Y
あ	ろ	い	ね	う	の	え	ふ	お	す
か	う	き	む	く	り	け	れ	こ	ら
さ	き	し	る	す	に	せ	か	そ	や
た	ん	ち	わ	つ	こ	て	そ	と	よ
な	い	に	あ	ぬ	も	ね	お	の	は
は	え	ひ	さ	ふ	て	へ	ま	ほ	く
ま	ゆ	み	け	む	め	め	ひ	も	し
や	み			ゆ	せ			よ	ぬ
ら	を	り	た	る	な	れ	ほ	ろ	へ
わ	ち							を	と
ん	つ								

この表は『あいうえお...』を適当に並べ換えたものです。とりあえず，濁点や『っゃゅょ』などは無視することにします。何か文があったら，それを平仮名で書き，上の表にしたがって，X 欄の文字を Y 欄の文字で置き換えると，意味の通じない文になります。例えば，

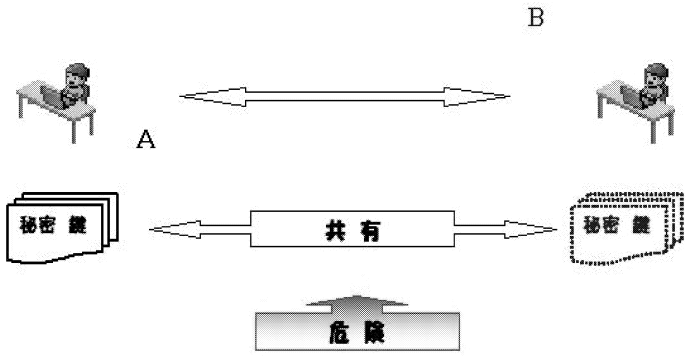
あすははれるとおもいます

という文をこの法則で変換してみると，

ろにええほなよすしねゆに

となります。最初の文を平文，後の文を暗号文といいます。暗号文があれば，表にしたがって，平文にすることもできます。その際には，表のＸ欄とＹ欄を逆にしてＹ欄を『あいうえお』順にしたものを作っておくということもできます。このように平文から暗号文を作ることを『暗号化』，暗号文から平文を作ることを平文の『復元』といいます。なお，第三者が暗号を破って情報を不正に得ることを暗号の『解読』といいます。

さて，この暗号を使って，Ａさんとさんという人が，他の人にわからないように何かの情報をやりとりするとします。Ａさんがさんに情報を伝えるとしたら，当然暗号文を送ることになるわけですが，さんがそれを平文に復元するためには，Ａさんと同じ上の表を持っていなければなりません。



暗号を作ったり，平文に復元したりするための情報を『鍵』といいますが，この場合は暗号を送る人と受け取る人が同じ鍵を共有しなければならないので，このような暗号のことを『共通鍵暗号』といいます。

さて，この暗号には安全上２つの問題があります。１つは共通鍵を知らなくても解読されやすいということです。『ろにええほなよすしねゆに』くらいの文を１回送るだけだったら問題はありませんが，送る情報量が増えると問題が生じます。それは，『あいうえお』が普通の文章の中で現れる割合が違うからです。上の文でも『え，に』が２回現れて他の文字は１回だけです。私は日本語の一般的な文章で『あいうえお』のなかでどの文字が一番多く現れるかは知りませんが，例えば英語では『e』という文字が一番多く現れることはよく知られています。だから，少し長い文章をこの方法で送ると，第三者がそれを傍受した場合，多く現れる文字が何であるか幾つか調べて，それを一般的に多く現れる文字で置き換える，というようなことができます。そして少しでも意味のある部分が出来たら，それは正しい置き換えということになりますか

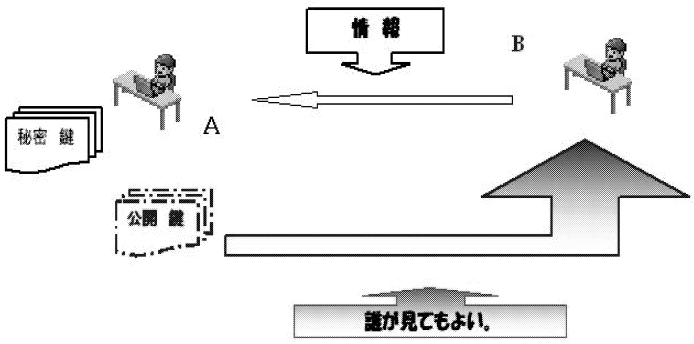
ら，それを手がかりにして，もっと調べる，というように芋ずる式に暗号を破られてしまいます。

もう1つの問題は，共通鍵をある段階で送らなければならないということです。友人どうしが遊びで情報をやりとりするために，家から家へ共通鍵を運ぶのなら問題はありませんが，国家機密をやりとりするために，共通鍵を1つの国からもう1つの国に運ぶというようなことになると，その共通鍵を運ぶ過程でそれを盗もうとする人も現れてくるかもしれません。あるいは，2つの銀行の間で経済的に重要な情報をやりとりする場合にも，共通鍵が盗まれる危険性があります。

このように，上のような暗号は，2つの理由で安全上問題があります。最初の問題は暗号の強度が強ければ問題ありませんが，共通鍵暗号の場合，共通鍵の傍受という問題が常にあります。そこで登場したのが『公開鍵』を使った暗号です。公開鍵暗号についてはこれからお話しますが，共通鍵暗号は現在でも使われています。共通鍵暗号でも，暗号自身の強度が高く，共通鍵さえ安全に伝えることが出来れば問題ありません。例えば，膨大な情報を通信したいというようなときには，共通鍵暗号のほうが公開鍵暗号よりも通信速度が速いので，共通鍵をいったん公開鍵暗号で伝えて，それから共通鍵暗号を使うなどということは一般的です。

2　公開鍵暗号

1976 年に Diffie 氏と Hellman 氏は第三者が傍受する可能性のある通信経路を想定して鍵を共有する DH 鍵共有という考え方を初めて提唱しました。それは，暗号そのものではありませんが，1977 年には，Rivest 氏，Shamir 氏，Adelman 氏によって現在広く使われている公開鍵暗号の1つである RSA 暗号というものが考案されました。まず公開鍵暗号の考え方を説明します。



公開鍵暗号とは，平文を暗号化するのと，暗号文から平文に戻すのに別の鍵を使うものです。大切な点は，公開鍵は誰が見てもよく，暗号を解読するのには，余分な情

報 (秘密鍵) が必要になるというものです。だから，A さんが B さんから情報を貰いたいというときには，まず A さんが公開鍵を B さんに伝えます。そして，B さんが公開鍵を使って暗号文を作り，A さんに伝えます。A さんは自分だけが持っている秘密鍵を使って暗号を解読し，それによって，B さんからの情報を得ます。ここで，A さんは秘密鍵を誰にも伝える必要がないので，暗号の安全性が高まります。このような暗号は銀行など，さまざまな金銭授受の場で使われています。

さて，公開鍵は誰でも見てよいわけですから，このような暗号は公開鍵から秘密鍵がわかるようなものでは暗号になりません。つまり，平文 X から暗号文 Y を作るときに，余分な情報がないと Y から X が作れないというようなものでなくてはならないということです。このように，X から Y という操作をするとき，Y から X へ戻すことが，余分な情報を持っていないと非常に難しいというような過程を『不可逆過程』といいます。

RSA 暗号は最初にそのような不可逆過程を実現した暗号です. 現在では RSA 暗号だけでなく,『楕円曲線暗号』といったさまざまな公開鍵暗号が知られています。

3　割算の余り

RSA 暗号について話す前に，少し整数の割算についてお話ししましょう。a, b が正の整数のとき，a を b で割った余りは必ず 0 から $b-1$ までの整数になります。

例 3.1.　(1) 20 は 5 で割り切れるので，20 を 5 で割った余りは 0 です。

(2) 5 を 3 で割った余りは 2 です。

(3) 58 を 11 で割った余りは 3 です。

負の整数についても割算を考えることができますが，今日は正の整数で割る場合だけ考えましょう。正の整数 a が整数 b を割り切るとき，a は b の約数，b は a の倍数といいます。1 より大きい整数 p の約数が 1 と p だけであるとき，p を素数といいます。

例 3.2.　(1) 2 の約数は $1, 2$ なので，2 は素数です。

(2) $3, 5, 7, 11, 13, 17, 19$ も素数です。

(3) 4 の約数は $1, 2, 4$ です。$1, 4$ 以外の約数があるので，4 は素数ではありません。4 は 2 の倍数です。

(4) 6 の約数は $1, 2, 3, 6$ です。6 は素数ではありません。

(5) 12 の約数は $1, 2, 3, 4, 6, 12$ です。12 は素数ではありません。

2 つの正の整数 a, b の共通の約数・倍数を公約数・公倍数といいます。公約数の中で一番大きいものを最大公約数といいます。公倍数の中で一番小さいものを最小公倍数といいます。最大公約数が 1 であるとき，a, b は互いに素であるといいます。

例 3.3. (1) $12, 16$ の公約数は $1, 2, 4$ です。だから最大公約数は 4 です。12 の倍数 $12, 24, 36, 48, \ldots$ の中で最初に 16 の倍数になるのは 48 ですから，48 が最小公倍数です。

(2) $14, 21$ の公約数は $1, 7$ で最大公約数は 7 です。最小公倍数は 42 です。

(3) $3, 4$ は互いに素です。

(4) 12 と 35 も互いに素です。

(5) 6 と 8 は 2 を共通の約数に持つので，互いに素ではありません。

$a = ma', b = mb'$ で m が a, b の最大公約数なら，a, b の最小公倍数は $ma'b'$ なので，ab の約数になっています。

整数の割算の余りは，和・差・積と整合性があることが知られています。つまり，a を正の整数，n, m を 0 以上の整数とするとき，n, m を a で割った余りを x, y とすると，$n+m, n-m, nm$ を a で割った余りはそれぞれ $x+y, x-y, xy$ を a で割った余りと等しいことがわかります。

例 3.4. $a = 7$, $n = 775, m = 72$ とします。このとき，n, m を 7 で割った余りは $5, 2$ です。だから，$n+m, n-m, nm$ を 7 で割った余りは $5+2 = 7, 5-2 = 3, 5 \times 2 = 10$ を 7 で割った余り，つまり $0, 3, 3$ になります。これは nm などを計算してから余りを求めるよりもずっと効率的です。

4 RSA 暗号の実際

RSA 暗号とはどのようなものかを説明するのに，例から始めることにします。数学を使って暗号化するので，平仮名に適当に番号をつけて，文字を整数に変換します。例えば，次のように数と対応させましょう。

あ	1	い	2	う	3	え	4	お	5
か	6	き	7	く	8	け	9	こ	10
さ	11	し	12	す	13	せ	14	そ	15
た	16	ち	17	つ	18	て	19	と	20
				っ	23				
な	26	に	27	ぬ	28	ね	29	の	30
は	31	ひ	32	ふ	33	へ	34	ほ	35
ま	36	み	37	む	38	め	39	も	40
や	41			ゆ	43			よ	45
ゃ	46			ゅ	48			ょ	50
ら	51	り	52	る	53	れ	54	ろ	55
わ	56	を	57	ん	58	゛	59	゜	60
。	61	,	62	空白	63				

この表により，文章は整数の列になります。例えば『きょうは，はれです。』という文なら

$$07, 50, 03, 31, 62, 31, 54, 19, 59, 13, 61$$

となります。ここで，これらの数字をそのまま暗号化しても，どのような暗号を使っても，結局出力は高々100 個くらいしかありません。これは並べ替えの暗号と結局同じことになってしまうので，これらの数字をそのまま使うことはしません。実際には，これを 400 桁くらいに分け直して使います。今日は原理を理解してもらいたいだけなので，3 桁づつに分け直します。すると

$$075,003 = 3,316,231,541,959,136,100$$

となります。 最後は半端なので，00 を付け加えました。

RSA 暗号ではこれを次のように暗号化したり，解読したりします。まず 2 つの素数 $29, 41$ を選び，$n = 29 \times 41 = 1189$ とします。実際には，200 桁くらいの非常に大きい素数を 2 つ使います。n で割った余りを使うので，3 桁の数を暗号化するなら，n は 4 桁以上の数でないと，違う数の余りが同じになってしまいます。n が 400 桁の数なら，399 桁の数を暗号化できます。$(29-1)\times(41-1) = 28\cdot 40$ と互いに素な整数，例えば $e = 3$ を選びます。 これで暗号を作るのに必要な情報は全てです。ここで，n と e が公開鍵で，$29, 41$ が秘密鍵になります。まとめると，次のようになります。

必要な情報のまとめ

公開鍵 $n = 1189$, $e = 3$　秘密鍵 $29, 41$

この場合は 1189 が与えられると，$1189 = 29\cdot 41$ いうことが簡単にわかるので，秘密鍵がわかってしまいます。しかし，n が 2 つの 200 桁くらいの素数の積の場合，現在わかったいる方法では，その 2 つの素数を見つけるのに天文学的な時間が必要なので，2 つの素数 p, q が秘密鍵の役割を果たせます。 だから，**将来非常に大きい整数を素数の積で表す方法が見つかれば，RSA 暗号は使えなくなります。**

これらの情報を使って，次のように暗号化します。

暗号化の作業

$0 \leqq x < 1189$ に対し，x^3 を 1189 で割った余りを $\phi(x)$ とする。

x が平文で $\phi(x)$ が暗号文です。暗号文を受け取る人は解読できなくてはいけないわけですが，p, q がわかっていると，もともとの x を求めることができることが知られています。これは次のように書いておきますが，後でもっと易しい状況のときに説明することにします。

定理 4.1. p, q を異なる素数，$n = pq$，e は $(p-1)(q-1)$ と互いに素な正の整数とする。整数 $0 \leqq x < n$ に対し，x^e を n で割った余りを $\phi(x)$ とする。このとき，正の整数 d が存在して，全ての整数 $0 \leqq x < n$ に対し，$\phi(x)^d$ を n で割った余りが x になる.

$n = 1189, e = 3$ なら，$d = 187$ と取れます。どうやってこの d を見つけるかということは後で説明することにして，この d で元に戻るということを説明します。これは次の**フェルマーの小定理**ということにもとづいています。

定理 4.2. (フェルマーの小定理) p が素数で $0 < x < p$ が整数なら，x^{p-1} を p で割った余りは 1 になる.

このことを使うと，$(x^3)^{187} = x^{561}$ なので，x が 29 でも 41 でも割り切れなければ,

$$x^{561} = (x^{28})^{20}x, \quad x^{561} = (x^{40})^{14}x$$

となり，x^{561} を 29 で割った余りと 41 で割った余りはそれぞれ x を 29 で割った余りと 41 で割った余りになることがわかります。このことを使うと，x^{561} を 1189 で割った余りが x を 1189 で割った余りになることをわかります。また，x が 29 や 41 で割り切れる場合にも同じことが成り立つことも，多少の考察によりわかります。

5 RSA 暗号の解読の作業

RSA 暗号を体験するために，もっと易しい状況で暗号文を実際に平文に復元してみましょう。RSA 暗号は実際には 2 つの素数の積 $n = pq$ を考えますが，3 桁の数のかけ算や割算は大変なので，1 つの小さい素数 $n = p$ を考えましょう。この場合には，もちろん暗号にはなりませんが，暗号の原理を理解するのには手頃だと思います。そこで，$n = p = 89$ とします。

$e = 59$ は $p - 1 = 88$ と互いに素な数です。この e に対し，$d = 3$ と取れることがわかります。実は暗号解読の作業が楽になるように，$d = 3$ になる e を求めたのですが，これについては後で解説します。

$$(x^{59})^3 = x^{177} = (x^{88})^2 x$$

なので，$0 \leqq x < 89$ なら，$(x^{59})^3$ を 89 で割った余りは x になります。

まとめると，

暗号化: $x \to x^{59}$ を 89 で割った余り
暗号解読: $x \to x^3$ を 89 で割った余り

となります。

実際の作業の例

実際に暗号解読の作業をしてみましょう。89 は 2 桁なので，2 桁の数をそのまま使います。ですから，この意味でも，実際には使えない暗号です。暗号文

$$21, 44, 40$$

を平文に復元してみましょう。

$$21 \times 21 = 441 = 4 \cdot 89 + 85, \quad 21 \times 85 = 1785 = 20 \cdot 89 + 5$$

となり，21 は 5 に対応します。同様にして

$$44 \times 44 = 1936 = 21 \cdot 89 + 67, \quad 44 \times 67 = 2948 = 33 \cdot 89 + 11,$$
$$40 \times 40 = 1600 = 17 \cdot 89 + 87, \quad 40 \times 87 = 3480 = 39 \cdot 89 + 9$$

となるので，平文は

$$5, 11, 9$$

つまり,『おさけ』です。

それでは皆さん，御自分で次の暗号文を平文に復元してみてください。

問題: 暗号文 $27, 19, 16$ を平文に復元せよ。

これには次のような表を使うと整理できます。

(1)	数	27
(2)	2 乗	
(3)	3 乗	

(1)	数	19
(2)	2 乗	
(3)	3 乗	

(1)	数	16
(2)	2 乗	
(3)	3 乗	

6 ユークリッドの互除法と d の見つけかた

$n = 89, e = 59$ のときには $d = 3$ であるといいましたが，e から d をどうやって見つけるかについてお話します。それには，ユークリッドの互除法というものを使います。

$(x^e)^d = x^{de}$ を割った余りが x になるような d を見つけるわけですが，$x^{de} = x^{ed}$ ですから，e から d を見つけるのも d から e を見つけるのも同じです。x が p の倍数なら，x^{de} も p の倍数なので，両方とも p で割った余りは 0 です。だから，x は p で割り切れないと仮定します。

もし $de - 1 = k(p-1)$ となるように d, k を見つけられれば，フェルマーの小定理によって，

$$x^{de} = x^{de-1}x = \left(x^{p-1}\right)^k x$$

を p で割った余りは x になります。

$e = 59$ なら，$59d - 88k = 1$ となるように d, k が見つけられればよいわけです。$a > b > 0$ を整数とします。a を b で割った余りを r とします。つまり，整数 c があり，$a = cb + r$ $(0 \leqq r < b)$ です。このとき，次の性質が成り立ちます。

定理 6.1. 上の状況で，a, b の最大公約数は b, r の最大公約数に等しい。

証明. d を正の整数とします。 d が a, b を割り切るなら，d は $a - cb$ も割り切ります。したがって d は b, r を割り切ります。よって a, b の最大公約数は b, r の最大公約数以下です。

逆に d が b, r を割り切るとします。$a = cb + r$ なので，d は a, b を割り切ります。したがって b, r の最大公約数は a, b の最大公約数以下です。 □

例 6.2. $12, 5$ の最大公約数を求めます。$12, 5$ が互いに素であることは明らかですが，上の定理を使って求めます。

$$12 = 2 \cdot 5 + 2,$$
$$5 = 2 \cdot 2 + 1$$

となるので，$12, 5$ の最大公約数は $5, 2$ の最大公約数と等しく，$2, 1$ の最大公約数，つまり 1 であることがわかります。

このような最大公約数の求めかたを**ユークリッドの互除法**といいます。a, b の最大公約数が m であるとき，$ax + by = m$ となる整数 x, y をユークリッド互除法により求めることができます。例えば上の例では

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 2 \cdot 5) \\ &= (-2) \cdot 12 + 5 \cdot 5 = (5 - 2) \cdot 12 + (5 - 12) \cdot 5 \\ &= 3 \cdot 12 - 7 \cdot 5 \end{aligned}$$

となります。

これを $88, 59$ に適用してみましょう。

$$88 = 59 + 29,$$
$$59 = 2 \cdot 29 + 1$$

となるので，

$$\begin{aligned} 1 &= 59 - 2 \cdot 29 = 59 - 2 \cdot (88 - 59) \\ &= 3 \cdot 59 - 2 \cdot 88 \end{aligned}$$

となり，$3 \cdot 59 = 2 \cdot 88 + 1$ であることがわかります。このように，$e = 59$ から $d = 3$ が求まりました。(実は $d = 3$ から $e = 59$ を求めました。)

$n = pq$ で e が $(p - 1)(q - 1)$ と互いに素な整数であるとき，すべての整数 x に対して，$(x^e)^d = x^{de}$ を n で割った余りが x を n で割った余りと等しいような d を見つけることができることを示します。これは $x^{de} - x$ が n で割り切れることを意味します。p, q は異なる素数なので，n で割り切れることと，p, q 両方で割り切れることは同じです。ですから，

$(*)$ 全ての x に対して，$x^{de} - x$ が p, q 両方で割り切れる

d を探すことになります。

L を $p-1, q-1$ の最小公倍数とします。L は $(p-1)(q-1)$ の約数です。e は $(p-1)(q-1)$ と互いに素なので，L とも互いに素です。だから，$de - kL = 1$ となる整数 d, k があります。しかもこの d はユークリッドの互除法を使って具体的に求めることができます。d に L を加え，k に e を加えてもこの等式は成立ちますから，$d, k > 0$ としてもかまいません。この d が求めるものであることを示します。

上の性質 $(*)$ を示します。同じことなので，p についてだけ示します。まず x が p で割り切れれば，x^{de}, x 両方 p で割り切れるので，$x^{de} - x$ は p で割り切れます。ですから，x は p で割り切れないとします。このとき，フェルマーの小定理により，x^{p-1} を p で割った余りは 1 です。ですから，$\left(x^{p-1}\right)^{k\frac{L}{p-1}}$ を p で割った余りも 1 になります。

$$x^{de} = x^{kL}x = \left(x^{p-1}\right)^{k\frac{L}{p-1}}x$$

なので，x^{de} を p で割った余りは x を p で割った余りと同じになり，$x^{de} - x$ は p で割り切れます。まとめると，次のようになります。

もし $n = pq$ となる p, q がわかっているとき，$p-1, q-1$ の最小公倍数を L として $de - kL = 1$ となる $d > 0$ をユークリッドの互除法を使って求めれば，この d で暗号文を平文に復元できる。

実際には p, q は非常に大きい素数ですから，$p-1, q-1$ の最小公倍数を見つけるのも労力が必要です。ですから，上で L の代わりに $(p-1)(q-1)$ を使ってもかまいません。

$n = 1189, e = 3$ の場合にも d を求めてみましょう。$p-1 = 28, q-1 = 40$ なので，最大公約数は 4, 最小公倍数は 560 です。

$$560 = 186 \cdot 3 + 2,$$
$$3 = 2 + 1$$

となるので,

$$1 = 3 - 2 = 3 - (560 - 186 \cdot 3) = 187 \cdot 3 - 560$$

となり，$d = 187$ と取れることがわかります。

このように　$n = pq$ が 2 つの素数の積の場合，p, q がわかれば e から d が求まります。p, q が非常に大きい場合，n から p, q を短時間で見つける方法は現在では見つかっていません。

7　高いべきの計算

実際に RSA 暗号を使うときには，整数 x のべき x^d を n で割った余りを計算することになりますが，d は n と同じくらい大きい数になることもあります。例えば d が

400 桁の数なら，このような計算はできるのでしょうか。答えは Yes です。これについて説明します。

もちろん x を 10^{400} 回かけるのには，天文学的な時間がかかります。けれども，工夫をすれば，短い時間で計算ができます。例を考えることにしましょう。40^{17} を 89 で割った余りを求めましょう。これを次のように計算します。

40^2 を 89 で割った余りは，87
40^4 を 89 で割った余りは，87^2 を 89 で割った余りに等しく，4
40^8 を 89 で割った余りは，4^2 を 89 で割った余りに等しく，16
40^{16} を 89 で割った余りは，16^2 を 89 で割った余りに等しく，78
40^{17} を 89 で割った余りは，78×40 を 89 で割った余りに等しく，5

ここでポイントは 40 を 17 回かけるよりもずっと速く計算ができたことです。このように $x^2, x^4, x^8, \ldots$ と計算していけば，常に割った余りを考えるので，n より小さい整数を考えることになり，また 2^k は k が大きくなると，非常に速く大きくなるので，x^d は d が大きくても比較的速く計算できます。上では 5 回で計算ができました。対数関数を知っている方はだいたい $\log d$ くらいの回数で計算ができるということがおわかりいただけるのではないでしょうか。

もちろん d が 400 桁の数なら，x^d を計算するのに 2000 回くらいの計算が必要になるかもしれませんが，それはコンピューターなら短時間でできることです。

8 問題 (宿題)

$n = 1189$, $e = 11$ という公開鍵で作った次の RSA 暗号を考えます。

$$190, 790, 510, 1175$$

この暗号を解読してください。この場合 $1189 = 29 \cdot 41$ となることを知っていますから，今日お話したことにより，元に戻すのに必要な d をユークリッドの互除法で見つけることができるはずです。d を見つけたら少し高いべきですが，工夫して計算できます。もしパソコンを持っていれば,『アクセサリ』の中の『電卓』を選んで，設定を『関数電卓』にすれば，`257^2 mod 1189` というふうにして，257^2 を 1189 で割った余りを求めることができます。

9 フェルマーの小定理の証明

少し技術的になりますが，フェルマーの小定理を証明しておきます。素数 p を固定します。

$$\binom{p}{n} = \frac{p(p-1)\cdots(p-n+1)}{n(n-1)\cdots 1}$$

は二項係数と呼ばれ整数です。$0 < n < p$ なら，分子は p で割り切れ，分母は p で割り切れないので，$\binom{p}{n}$ は p で割り切れる整数です。二項定理により，

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1}y \cdots + \binom{p}{p-1} xy^{p-1} + y^p$$

なので，$(x+y)^p - x^p - y^p$ は p で割り切れます。

補題 9.1. $x^p - x$ は p で割り切れる。

証明. p で割った余りだけが問題なので，$x = 0, \ldots, p-1$ と仮定してかまいません。

$x = 0, 1$ については明らかに成り立っています。$x = k$ に対して成り立てば，$y = k+1$ に対して，

$$y^p - k^p - 1 = y^p - x^p - 1$$

は p で割り切れますが，$x^p - x$ は p で割り切れるので，$y^p - x - 1 = y^p - y$ は p で割り切れます。 □

補題 9.2. x が p で割り切れなければ，整数 y があり，xy を p で割った余りが 1 になる。

証明. 整数 y, n で $yx - np = 1$ となるものがあります。m に p を足し，n に x を足してもこの等式は成り立つので，$y, n > 0$ としてかまいません。すると，yx を p で割った余りは 1 になります。 □

フェルマーの小定理の証明. 補題 9.1 により，$x^p - x$ は p で割り切れます。補題 9.2 により，yx を p で割った余りが 1 になるような正の整数 y があります。$yx^p - yx = yx(x^{p-1} - 1)$ は p で割り切れますが，yx を p で割った余りは 1 なので，$x^{p-1} - 1$ は p で割り切れます。 □

補題 9.2 は p で割った余りの集合が『群』になるということを主張しています。フェルマーの小定理は『群の元の位数は群の元の個数の約数である』という『ラグランジュの定理』というものの特別な場合になっています。