剰余演算と RSA 暗号

～背景となる数学の定理～

全体像の把握

RSA 暗号を理解する上で、必要な要素を列挙すると以下のようになる。

- 合同式
- オイラーの定理
- 拡張ユークリッド互除法

オイラーの定理が、RSA 暗号の核心である。それを理解するためには合同式を理解している必要がある。ここまで理解できれば、暗号化と復号がうまくいく理由がおおよそわかるだろう。拡張ユークリッド互除法は、秘密鍵をいい感じにとってくるために利用する。

このことを念頭に置いて本教材で学習を進めてほしい。

1 合同式

1.1　合同式の導入

具体例で考えてみる。ありとあらゆる整数を 3 で割ってみてほしい。すると、その余りが 0, 1, 2 となるグループにすべての整数を重複なく分類できることがわかるだろう。ここで、余りは、0 以上割る数未満の整数でとる（最小非負剰余）。例えば-5 を例にとると、-5 = 3×(-2) + 1 であるから、余りは 1 とみる。

ある整数で割った余りに着目するのが「合同」の考え方である。

定義 1

nを 2 以上の整数とする。

「二つの整数a, bがnを法として合同」であるとは、aをnで割った余りとbを n で割った余りが等しいことをいい、次のように表す。

$$a \equiv b \ (mod\ n)$$

例えば、法を 5 としたとき、$6 \equiv 11 \ (\mathrm{mod}\ 5)$である。

1.2　合同式の性質

以下に示す、足し算と掛け算に関する合同式の性質を理解することは、合同式の考え方に対する理解を深めるとともに、今後登場する RSA 暗号の背景にある定理を理解する上で大変重要である。

定理 1-1

nを自然数とし、a, b, c, dを整数とするとき、(1)～(3)が成り立つ。

(1)　$a \equiv b \ (mod\ n), c \equiv d \ (mod\ n) \ \Rightarrow a + c \equiv b + d \ (mod\ n)$

(2)　$a \equiv b \ (mod\ n) \ \Rightarrow ac \equiv bc \ (mod\ n)$

(3)　$ac \equiv bc \ (mod\ n) \Rightarrow a \equiv b \ (mod\ n)$（$c$は$n$と互いに素）

※互いに素とは、両者の最大公約数が 1 であることをいう。

Proof:

(1)を証明する。$a \equiv b \ (mod\ n), c \equiv d \ (mod\ n)$とすると、1 つ目の条件から、$a$と$b$は$n$で割った余りが等しいため、その余りを$r$とすると、ある整数$k, l$により

$$a = kn + r, b = ln + r$$

と表される。同様に、2 つ目の条件より、c, dをnで割った余りは等しく、その余りをr'とすると、ある整数p, qにより

$$c = pn + r', d = qn + r'$$

と表される。最終的に示したいことは、$a + c$を n で割った余りと、$b + d$を n で割ったあまりが等しいことであるから、それぞれを上記の表現により書き出してみる。すると

$$a + c = (k + p)n + (r + r'),$$

$$b + d = (l + q)n + (r + r')$$

よって、両者の n で割った余りは等しいため、$a + c \equiv b + d\ (mod\ n)$がいえる。

(2)を証明する。仮定するのは 1 における 1 つ目の条件と同じであるから、それを流用すると

$$a = kn + r, b = ln + r$$

であるが、上式のそれぞれの両辺に整数cを乗じて

$$ac = (kc)n + cr,$$

$$bc = (lc)n + cr$$

を得る。従って、acとbcは、nで割った余りが等しいため、$ac \equiv bc\ (mod\ n)$がいえる。

(3)を証明する。$ac \equiv bc\ (mod\ n)$より、今までと同様、ある整数k, l, rが存在して

$$ac = kn + r,\ \ bc = ln + r$$

と表される。よって、$ac - bc = c(a - b) =\ (k - l)n$

cとnは互いに素より、cはnで割り切れない。なおかつ、上式より$c(a - b)$はnの整数倍で表現されるのだから、$a - b$がnの倍数であることがわかる。これはつまり、$a - b$がnで割り切れるということであり、合同式で表現すると、$a - b \equiv 0\ (mod\ n)$ である。両辺にbを足して

$$a \equiv b\ (mod\ n)$$

を得る。

注意: 上記の合同式の両辺にbを足す操作は、$a - b \equiv 0\ (mod\ n),\ b \equiv b\ (mod\ n)$ なる 2 つの合同式を用意して、定理 1-1 を適用していることに他ならない。

Q.E.D.

1.3 暗号と結びつける

スライド資料に示した古典暗号のひとつ「シーザー暗号」は、合同式を利用することで式として表現可能である。まず、A を 0、B を 1、C を 2、・・・、Z を 25 と対応させ、以降アルファベットは置き換えた数字で考えることにする。 1 文字からなる平文をmとし、鍵（何文字ずらすか）をk、暗号文をcとすると

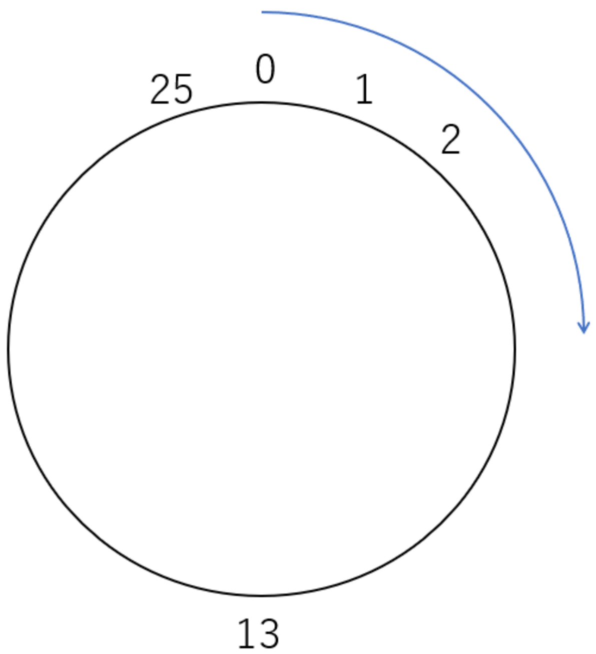
$$c \equiv m + k\ (mod\ 26)$$

となる（ただし、$0 \leq c \leq 25$）。
復号の際は、先ほど平文mに対して鍵kを作用させた分をもとに戻したいので、
$k + x \equiv 1\ (mod\ 26)$を満たす$x$を更に足すことで$m$に戻せばよい。すなわち、$x = 26 - k$とすればよい。なぜならば、mod26 で考えるときは 26 を足して一巡するので、そこからkを引けば$x > 0$を足す操作により、$k + x \equiv 1$が実現されるためである。

$$m \equiv c + x = (m + k) + (26 - k) = m + 26\ (mod\ 26)$$

が復号の内訳である。

例えば、$m = 0,\ k = 2$ というシーザー暗号を考えると、下図において、0 を 2 つ分ずらした 2 が暗号文となる。暗号化も復号も時計回り（足し算）で考えるから、復号したければ 26 を足してから 2 を引けば元に戻る。つまり、mod26 の世界では 2 に対して$26 - 2$を足すと 0 と合同（26 はもちろん 26 で割り切れる）になり、元に戻る。



2 オイラーの定理

本章では、オイラーの定理を、RSA 暗号で利用される形でのみ導入することを目標とする（一般のオイラーの定理を導入すると、RSA 暗号を速習するという趣旨から逸れてしまうと判断したため）。以降、そのオイラーの定理の特殊形を、単にオイラーの定理と呼ぶことにする。

オイラーの定理を証明するために必要な補題、定理を導入してゆく。

補題 2-1

aとpを互いに素な整数とする。このとき、

$a,\ 2a, \cdots,\ (p-1)a$ という、$p-1$個の整数をpで割った余りはすべて異なる。

Proof:

背理法で証明する。すなわち、$k \neq l$でありながら、kaとlaをpで割った余りが等しいようなk, l（$= 1, 2, \cdots, p-1$）が存在すると仮定して矛盾を導く（ここでは、$k > l$ とする)。

仮定より、

$$ka \equiv la\ (mod\ p)$$

を得る。aとbが互いに素であるから、定理 1-1(3)を適用すると

$$k \equiv l\ (mod\ p)$$

となる。しかし、上式が成り立つためには、仮定した状況においては$k = l$でなければならず、$k \neq l$に矛盾する。

したがって、補題 2-1 は成り立つ。

Q.E.D.

定理 2-1（フェルマーの小定理）

pを素数、aをpと互いに素な整数とするとき、

$$a^{p-1} \equiv 1\ (mod\ p)$$

が成り立つ。

Proof:

pを素数、aをpと互いに素な整数とする。このとき、補題 2-1 より、$a,\ 2a, \cdots,\ (p-1)a$ という、$p-1$個の整数をpで割った余りはすべて異なる。すなわち、それらの余りは 1, 2, ⋯, p-1 をすべてとる。よって、

$$a \cdot 2a \cdot \cdots \cdot (p-1)a\ \equiv 1 \cdot 2 \cdot (p-1)\ (mod\ p)$$

すなわち、

$$(p-1)!\cdot a^{p-1} \equiv (p-1)!\,(mod\ p)$$

したがって、

$$(p-1)!\ \cdot (a^{p-1}-1)\ \equiv 0\ (mod\ p)$$

ここで、$(p-1)!$はpで割り切れないので、$a^{p-1}-1$がpで割り切れる。
すなわち、

$$a^{p-1}-1\ \equiv 0\ (mod\ p)$$

よって、導くべき等式

$$a^{p-1} \equiv 1\ (mod\ p)$$

を得る。
Q.E.D.

補題 2-2
a,b,cを整数とする。
このとき、
　cはaと互いに素かつ、bとも互いに素$\Longrightarrow c$はabと互いに素
が成り立つ。

Proof:
　対偶を証明する。「cはabと互いに素でない」とすると、abは、cの素因数のうちの一つpで割り切れることになるので、aかbのうち、少なくともどちらか一方はpで割り切れる。よって、「cはaと互いに素でない、または、cはbと互いに素でない」となりり、対偶が真であるといえる。したがって補題 2-2 は成り立つ。
Q.E.D.

　ここまでで準備が整ったため、オイラーの定理を示す。

定理 2-2（オイラーの定理）
p,qを素数とする。
どんな自然数a,kに対しても

$$a^{k(p-1)(q-1)+1} \equiv a\ (mod\ pq)$$

が成り立つ。

Proof:
　aとp,qとの関係性で場合分けし、すべての場合において成り立つと示すことを証明の方針とする。

Case(1): aが、pとqのどちらとも互いに素な場合

補題 2-2 より、aはpqと互いに素である。また、仮定の一部「aはpと互いに素」より、フェルマーの小定理の適用条件を満たすので次が成り立つ。

$$a^{p-1} \equiv 1 \ (mod\ p)$$

両辺を$q-1$乗して

$$a^{(p-1)(q-1)} \equiv 1 \ (mod\ p) \ \cdots \ ①$$

を得る。また、仮定の一部「aはqと互いに素」に着目して同様に議論すると

$$a^{(p-1)(q-1)} \equiv 1 \ (mod\ q) \ \cdots \ ②$$

を得る。①と②より、ある整数k, lによって

$$a^{(p-1)(q-1)} = kp + 1 \ \cdots \ ①'$$

$$a^{(p-1)(q-1)} = lq + 1 \ \cdots \ ②'$$

と表せる。①′と②′から、$a^{(p-1)(q-1)} - 1$ はpの倍数でありながら、qの倍数でもある（要するにpとqのどちらでも割り切れる）ことがわかる。

よって、$a^{(p-1)(q-1)} - 1$ はpqで割り切れる（※1 : p, qが素数だから成り立つ命題)。そのことを合同式で表現すると

$$a^{(p-1)(q-1)} - a \equiv 0 \ (mod\ pq)$$

両辺にaを足して

$$a^{(p-1)(q-1)} \equiv 1 \ (mod\ pq)$$

両辺をk乗して

$$a^{k(p-1)(q-1)} \equiv 1 \ (mod\ pq)$$

両辺をa倍して

$$a^{k(p-1)(q-1)+1} \equiv a \ (mod\ pq)$$

Case(2): aが、p, qのうちのどちらかの倍数であり、もう一方とは互いに素な場合

aがpの倍数、qとは互いに素という状況で考えることにする。

aとqが互いに素より、フェルマーの小定理を適用すると

$$a^{q-1} \equiv 1 \ (mod\ q)$$

両辺を$k(p-1)$乗して

$$a^{k(p-1)(q-1)} \equiv 1 \ (mod\ q)$$

両辺をa倍して

$$a^{k(p-1)(q-1)+1} \equiv a \ (mod\ q)$$

すなわち、ある整数kによって

$$a^{k(p-1)(q-1)+1} = kq + a$$

よって、

$$a^{k(p-1)(q-1)+1} - a = kq$$

要するに、左辺はqで割り切れるということなのであるが、aはpの倍数なので、左辺はpでも割り切れる。よって、左辺はpqで割り切れる。このことを合同式で表現すると

$$a^{k(p-1)(q-1)+1} - a \equiv 0\ (mod\ pq)$$

両辺にaを足して

$$a^{k(p-1)(q-1)+1} \equiv a\ (mod\ pq)$$

Case(3): aが、pの倍数かつqの倍数である場合

　このとき、aはpqの倍数である（pqで割り切れる）ので、

$$a^{k(p-1)(q-1)+1} \equiv a\ (mod\ pq)$$

なぜならば、aを何乗しようとも、pqで割り切れるのだから、「割り切れる（余り 0)」という意味で合同がいえるからである。

以上、Case(1)〜Case(3)より、すべての場合について定理が成り立つことがいえた。

Q.E.D.

（※1 について）

示すべき命題:

　p,qを互いに異なる素数とするとき、 あらゆる整数mについて、mがpの倍数かつqの倍数ならば、mはpqの倍数である。

Proof:

　mがpの倍数かつqの倍数より、ある整数k,lが存在して、

$$m = kp = lq\ \cdots\ ①$$

となる。

$kp = lq$に着目して、両辺が等しいのだから、lもしくはqのどちらかは、pを素因数として持つことがわかる。しかし、pとqは互いに異なる素数との仮定より、qはpを素因数として持たない（素数の定義から直ちにわかる）。すなわち、lがpを素因数に持つ。よって、ある整数rが存在して、

$$l = rp\ \cdots\ ②$$

となる。①のうち、$m = lq$に着目して②を代入すると

$$m = rpq$$

を得る。

したがって、mがpqの倍数である。

Q.E.D

3 拡張ユークリッド互除法

ある２つの自然数a, bの最大公約数（dとおくことにする）を求め、

$$ax + by = d$$

を満たす整数の組(x, y)は、拡張ユークリッド互除法により、求めることができる。

一般的な書籍においては、最大公約数を求めるユークリッド互除法から導入し、それを文字通り拡張する形で、拡張ユークリッド互除法を示すという流れのものが多いが、それでは、証明に用いる記号をいちいち参照しなおしたりする手間があると考え、本教材では、拡張ユークリッド互除法を直接導入することにした。

定理 3-1（拡張ユークリッド互除法）

a, bを、$a > b$を満たす自然数とする。

$n_0 = a$，$n_1 = b$とし、$n_{i+2} = n_i \ mod \ n_{i+1} \ (i = 0, 1, 2, \cdots)$ とする。

上記の操作を繰り返してゆくと、あるところで、$n_s = 0$となる。

このとき、その一つ前であるn_{s-1}が、a, bの最大公約数に一致する。

また、n_iをn_{i+1}で割った商をq_{i+1}とし、

$$x_0 = 1,\ y_0 = 0,$$

$$x_1 = 0,\ y_1 = 1,$$

$$x_{i+2} = x_i - q_{i+1}x_{i+1},\ y_{i+2} = y_i - q_{i+1}y_{i+1}$$

によって、x_i, y_iを定める。

このとき、

$$ax_i + by_i = n_i$$

が成り立つ。

Proof:

１つ目の主張を証明する。

n_iをn_{i+1}で割った商をq_{i+1}、余りをn_{i+2}とおいたので、

$$n_i = q_{i+1}n_{i+1} + n_{i+2} \ \cdots ①$$

n_{i+1}とn_{i+2}のあらゆる公約数をcとおいて考えると、①より、n_iはcで割り切れる。

よって、n_{i+1}とn_{i+2}のあらゆる公約数cは、n_iとn_{i+1}の公約数である（図 1）。

また、n_iとn_{i+1}の、あらゆる公約数をdとおいて考えると、①より、

$$n_{i+2} = n_i - q_{i+1}n_{i+1}$$

なので、n_{i+2}はdで割り切れる。

よって、n_iとn_{i+1}のあらゆる公約数dは、n_{i+1}とn_{i+2}の公約数である（図 2）。

よって、$c = d$である（n_iとn_{i+1}の公約数と、n_{i+1}とn_{i+2}の公約数は等しい）$\cdots$ ②

②は、あらゆる公約数についての主張より、特に最大公約数についてもいえる。
したがって、

$$\gcd(n_i, n_{i+1}) = \gcd(n_{i+1}, n_{i+2}) \ \cdots \ ③$$

ただし、$\gcd(a, b)$はa, bの最大公約数を表す。
更に、n_0をn_1で割った余りn_2はn_1より小さな整数、n_1をn_2で割った余りn_3はn_2よりも小さな整数、・・・ となるので、n_iはiが増えるごとに小さくなってゆくことがわかる。
よって、

$$n_0 > n_1 > n_2 > \cdots \geq 0 \ \cdots \ ④$$

④より、どこかで$n_s = 0$となる。
ここで、③により、

$$\gcd(n_0, n_1) = \gcd(n_1, n_2) = \cdots = \gcd(n_{s-1}, n_s) = \gcd(n_{s-1}, 0) = \ n_{s-1} \ \cdots \ ⑤$$

がいえるが、$n_0 = a$, $n_1 = b$であったので、⑤から

$$\gcd(a, b) = \ n_{s-1}$$

である。

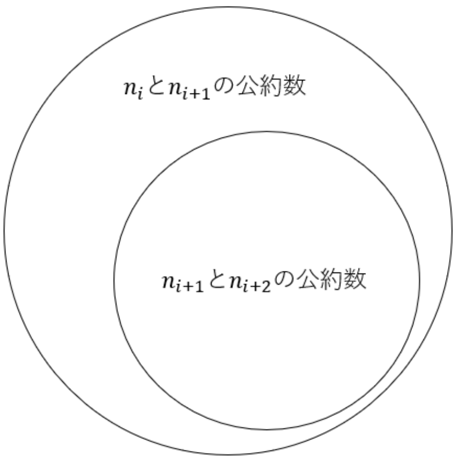


図1

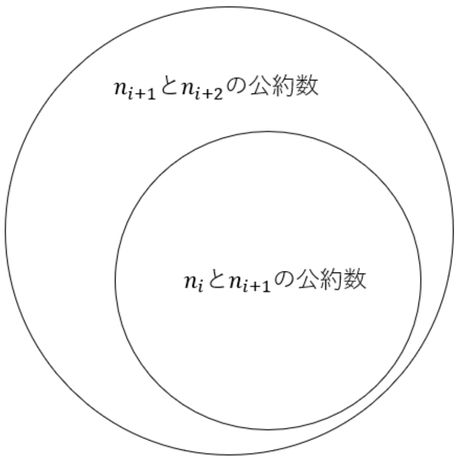


図2

２つ目の主張を、数学的帰納法により証明する。
$i = 0$のとき、$ax_i + by_i = \ ax_0 + by_0 = a = \ n_0$ より、成り立つ。
$i = 1$のとき、$ax_i + by_i = \ ax_1 + by_1 = b = \ n_1$ より、成り立つ。
$k = 0, 1, 2, \cdots$ に対して、

$$ax_k + \ by_k = \ n_k$$

$$ax_{k+1} + \ by_{k+1} = \ n_{k+1}$$

が成り立つと仮定すると、

$$\begin{aligned} &ax_{k+2} + by_{k+2} \\ &= a(x_k - q_{k+1}x_{k+1}) + b(y_k - q_{k+1}y_{k+1}) \end{aligned}$$

$$= (ax_k + by_k) - q_{k+1}(ax_{k+1} + by_{k+1})$$
$$= n_k - q_{k+1}n_{k+1}$$
が導かれる。
よって、すべての$i = 0, 1, 2, \cdots$ に対して
$$ax_i + by_i = n_i$$
が成り立つ。
Q.E.D.