RSA暗号の数理

新居俊作

2023 年 4 月 17 日

古来から離れた相手に他人に傍受される恐れのある手段で情報を伝えるためには暗号が使われている。

通常の暗号は、同じ「鍵」を使って暗号化と復号を行い、情報の送り手と受け手の間で安全な方法 (例えば手渡し) で事前に鍵を共有しておく。しかし、ネット通販等で顧客がネットショップ側に個人情報やクレジットカード番号などを送るには、事前に鍵を安全な方法で共有することができない。そのために開発された方法が「公開鍵暗号」である。この方法は、暗号化する「公開鍵」と復号する「秘密鍵」を別にし、暗号化のための公開鍵のみを知っていても暗号化された情報を復号出来ないようにしている。これにより、ネットショップは公開鍵を「公開」し、顧客はそれを用いて個人情報を暗号化して送ることにすると、第三者に傍受されても送った情報を盗み見られる危険がない。

本講で解説する RSA 暗号の開発により、この様な「公開鍵暗号」が一般に使われる様になった。

1　初等整数論

この節では、高等学校で習う整数の性質を前提に、RSA 暗号の原理を理解するために必要な初等整数論の知識をまとめる。

定義 1. n を正の整数とし a,b を整数とする。a を n で割った余りと b を n で割った余りが等しいとき a と b は n を法として合同であるといい

$$a \equiv b \ (\mathrm{mod}\ n)$$

と書く。

記号 整数 m が整数 n で割り切れることを $n|m$ と書き、割り切れないことを $n \nmid m$ と書く。

注意 1. $a \equiv b \pmod{n} \iff n|(a-b)$

定理 1. n を正の整数とし、a, b, c を整数とするとき、合同式 $\equiv$ は以下を満たす：

(1) $a \equiv a \pmod{n}$ (反射律)

(2) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$ (対称律)

(3) $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$ (推移律)

証明. (1)、(2) は明らか。
(3) について。

$$a \equiv b \pmod{n} \text{ かつ } b \equiv c \pmod{n} \iff n|(a-b) \text{ かつ } n|(b-c)$$

だが、$a - c = (a - b) + (b - c)$ なので、このとき $n|(a-c)$、つまり $a \equiv c \pmod{n}$。 □

定理 2. n を正の整数とし a, a', b, b' を整数とする。
$a \equiv a' \pmod{n}$ かつ $b \equiv b' \pmod{n}$ のとき以下が成り立つ：

(1) $a \pm b \equiv a' \pm b' \pmod{n}$ (復号同順)

(2) $a \cdot b \equiv a' \cdot b' \pmod{n}$

(3) $a^k \equiv (a')^k \pmod{n}$, $(k = 1, 2, \ldots)$

証明.

(1) $(a \pm b) - (a' \pm b') = (a - a') \pm (b - b')$ より従う。

(2) $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b')$ より従う。

(3) (2) より従う。

□

定理 3. n を正の整数とし、c を n と互いに素な整数とするとき、整数 a, b について

$$ac \equiv bc \pmod{n} \implies a \equiv b \pmod{n}$$

証明. $ac \equiv bc \pmod{n} \iff n|(ac-bc)$ だが、$ac-bc=c(a-b)$ で c が n と互いに素なので $n|(a-b)$。つまり $a \equiv b \pmod{n}$ □

定義 2. n を正の整数とするとき、$1 \leq i \leq n$ の範囲にある n と互いに素な整数 i の個数を $\varphi(n)$ と書き、オイラー関数とよぶ。すなわち

$$\varphi(n) = \#\{i \in \mathbb{Z} \mid 1 \leq i \leq n,\ i \text{ と } n \text{ は互いに素}\}$$

注意 2. p を素数とすると、そのオイラー関数の値は次で与えられる：

$$\varphi(p) = p - 1$$

定理 4. a, b を互いに素な正の整数とするときのオイラー関数は次を満たす：

$$\varphi(ab) = \varphi(a)\varphi(b)$$

証明. a 以下で a と互いに素な正の整数は $\varphi(a)$ 個ある。

α をその一つとし、$\alpha + ka$ の形の ab 以下の整数を考える。その様な整数は $\alpha, \alpha+a, \alpha+2a, \ldots \alpha+(b-1)a$ の b 個ある。これらの整数は a で割ると α 余るので a と互いに素である。

今 $\alpha + ka \equiv \alpha + la \pmod{b}$ とすると、$ka \equiv la \pmod{b}$ となるが、a と b は互いに素なので定理3より $k \equiv l \pmod{b}$ となり、$0 \leq k, l \leq b-1$ より $k = l$ である。従って、$\alpha, \alpha+a, \alpha+2a, \ldots \alpha+(b-1)a$ の形の整数を b で割った余りは互いに異なる。つまり、b で割った余りは 0 から $b-1$ までが一つずつ全てある。従って、この中で b と互いに素なもの数は $\varphi(b)$ 個である。(他の $b-\varphi(b)$ 個については、余りが 0 であるか、b で割った余りと b が互いに素ではないので、元の $\alpha+ka$ 自体も b と互いに素ではない。)

これは a と互いに素な全ての α について言えるので、a とも b とも互いに素な ab 以下の整数は全部で $\varphi(a)\varphi(b)$ 個ある。a と b は互いに素なので a とも b とも互いに素な整数は ab とも互いに素であるので結論が得られる。 □

補題 1. p を素数 $m_1, m_2, \ldots m_n$ を整数とすると

$$\left\{\sum_{k=1}^{n} m_k\right\}^p \equiv \sum_{k=1}^{n} m_k^p \pmod{p}$$

証明. 二項定理より $p|\{(m_1+m_2)^p-(m_1^p+m_2^p)\}$ であることを繰り返し用いる。 □

定理 5 (フェルマーの小定理)**.** p を素数とし、a を整数とすると

(1) $a^p \equiv a \pmod{p}$

(2) a と p が互いに素なら $a^{p-1} \equiv 1 \pmod{p}$

証明. 補題 1 で $m_1 = m_2 = \cdots = m_{|a|} = \pm 1$ とすると $a^p \equiv a \pmod{p}$ つまり $p|(a^p - a)$。

さらに p と a が互いに素なら、$a^p - a = a(a^{p-1}-1)$ なので、$p|(a^{p-1}-1)$ で $a^{p-1} \equiv 1 \pmod{p}$。 □

定理 6. n, t を正の整数、a を整数とし、n は平方因子を持たない (素数の二乗を約数に持たない) とし、$n = p_1 p_2 \cdots p_r$ と素因数分解されたとする。(n は平方因子を持たないので $i \neq j$ なら p_i と p_j は互いに素。) このとき

$$t \equiv 1 \pmod{(p_i - 1)} \Longrightarrow a^t \equiv a \pmod{p_i} \tag{1.1}$$

$$t \equiv 1 \pmod{\varphi(n)} \Longrightarrow a^t \equiv a \pmod{n} \tag{1.2}$$

証明.

(1) $t \equiv 1 \pmod{(p_i-1)} \iff p_i - 1 | t - 1$ より $t = (p_i - 1)k + 1$ となる 0 以上の整数 k がある。

(a) p_i と a が互いに素の場合

定理 5 (2) より

$$a^{p_i - 1} \equiv 1 \pmod{p_i}$$

この両辺を k 乗して a をかけると

$$a^{(p_i-1)k+1} \equiv a \pmod{p_i}$$

(b) p_i と a が互いに素ではないとき

p_i は素数なので $p_i | a$ なので $a^t \equiv 0 \pmod{p_i}$, $a \equiv 0 \pmod{p_i}$ で両辺 0 で成り立つ。

(2) 先ず、定理 4 を繰り返し使うと

$$\varphi(n) = \varphi(p_1 p_2 \cdots p_r) = \varphi(p_1)\varphi(p_2)\cdots\varphi(p_r)$$

である。

仮定より

$$\begin{aligned} t - 1 &= k\varphi(n) \\ &= k\varphi(p_1)\varphi(p_2)\cdots\varphi(p_r) \\ &= k(p_1 - 1)(p_2 - 1)\cdots(p_r - 1) \end{aligned}$$

従って $p_i - 1 | t - 1$ つまり $t \equiv 1 \pmod{(p_i - 1)} \quad (i = 1, 2, \ldots, r)$

よって (1) より $a^t \equiv a \pmod{p_i}$ つまり $a^t - a$ は p_i の倍数である $(i = 1, 2, \ldots r)$。これは $a^t - a$ が $p_1, p_2, \ldots p_r$ の最小公倍数 n の倍数であることを意味するので、$n | a^t - a$ となり $a^t \equiv a \pmod{n}$ となる。

□

定理 7 (中国の剰余定理)**.**

n_1, n_2 を互いに素な正の整数とする。

任意の整数 a_1, a_2 に対し、$x \equiv a_i \pmod{n_i}$ $(i = 1, 2)$ が成り立つような整数 x が存在する。

証明.

任意の整数 k について $x = kn_1 + a_1$ の形の整数は $x \equiv a_1 \pmod{n_1}$ を満たす。この x について

$$x = kn_1 + a_1 \equiv a_2 \pmod{n_2} \Longleftrightarrow kn_1 \equiv a_2 - a_1 \pmod{n_2}$$

が成り立つためには

$$kn_1 - (a_2 - a_1) = ln_2 \quad \text{つまり} \quad kn_1 - ln_2 = a_2 - a_1 \tag{1.3}$$

となる整数 l が存在すれば良いが、n_1 と n_2 は互いに素なので、この条件を満たす整数 k と l はユークッリドの互除法で求まる。 □

注意 3.

定理 7 で特に $0 \leq a_i < n_i$ $(i = 1, 2)$ のときは $0 \leq x < n_1 n_2$ となるように x を選ぶことができる。

証明.

上で求めた k を n_2 で割った商を m とするとき、$n_2n_1 - n_1n_2 = 0$ の m 倍を (1.3) の両辺から引くことによって $0 \leq k < n_2$ とすることができる。従って、

$$x = kn_1 + a_1 \leq (n_2 - 1)n_1 + a_1 = n_1n_2 - n_1 + a_1 < n_1n_2$$

□

2 RSA 暗号の原理

受け手が公開鍵を決める

(1) 十分大きな二つの素数 p, q $(p \neq q)$ を選び、$n = pq$ として、n から p, q を計算することが実用上必要な時間内にできない*ようにする。

(2) e と $\varphi(n)$ が互いに素であるような 2 以上の整数 e を求める。

上で決めた n, e を公開鍵とする。

受け手が使う復号鍵を求める

$ed \equiv 1 \pmod{\varphi(n)}$ を満たす正の整数 d を求める。

この d が復号鍵 (秘密鍵) となる。

送り手による暗号化

n より小さい正の整数 A を送るとする。

$A' \equiv A^e \pmod{n}$ となる A' を計算する。(A^e を n で割った余りが A'。)

この A' を暗号として受け手に送る。

---

*「コンピュータの基礎理論」[新居] の授業で述べるように、現在通常使われている計算機の原理に従うと、与えられた整数 n の素因数分解には 2^n の時間がかかるので、n を十分大きくすると実用的な時間内には計算出来ない。

しかし、1994 年に Shor によって、量子力学の原理を用いる計算機を使った場合の計算時間は n の多項式で表され、n をかなり大きくしても実用的な時間内で計算出来ることが証明されている。[Shor]

量子力学の原理を用いる量子計算機は長らく基礎研究が続いていたが、2011 年に最初の実用化がなされ急速に商用開発の段階に入っている。

受け手による復号

$A \equiv (A')^d \pmod{n}$ が成り立つので A が復元できる。

復号できることの証明.

$A' \equiv A^e \pmod{n}$ の両辺を d 乗すると $(A')^d \equiv A^{ed} \pmod{n}$

n は平方因子を持たず $ed \equiv 1 \pmod{\varphi(n)}$ なので、定理 6 (2) より $A^{ed} \equiv A \pmod{n}$ が成り立つ。

□

問題 1. 実際に $p = 3, q = 13$ の時に上の手順に従って e, d を決め (e は条件を満たす最小の整数を取れ)、$A = 30$ を暗号化し、それを復号できることを計算して確認せよ。

但し、例えば同じパスワードを複数のサイトで使い回すことは危険である。

例えば、公開鍵のうち n は互いに異なるが、e が共通であるような複数のサイトで同じパスワードを使い回し、それらが傍受されたとする。このときパスワードは暗号化されたデータのみから以下のように復元できる。

e を正の整数とし $n_1, n_2, \ldots, n_e$ を互いに素な正の整数とする。

$n_1, n_2, \ldots, n_e$ より小さい正の整数 A について $A^e \equiv A_i \pmod{n_i}$ $(i = 1, 2, \ldots, e)$ とするとき、以下のようにして A を求めることができる。

n_1 と n_2 が互いに素なので定理 7 と注意 3 より

$$x_1 \equiv A_1 \pmod{n_1} \quad \text{かつ} \quad x_1 \equiv A_2 \pmod{n_2}$$

となる整数 x_1 で $0 \leq x_1 < n_1 n_2$ を満たすものをユークリッドの互除法で求めることができる。

同様に $n_1 n_2$ と n_3 は互いに素なので

$$x_2 \equiv x_1 \pmod{n_1 n_2} \quad \text{かつ} \quad x_2 \equiv A_3 \pmod{n_3}$$

となる整数 x_2 で $0 \leq x_2 < n_1 n_2 n_3$ を満たすものを求めることができる。$x_2 - x_1$ は $n_1 n_2$ の倍数なので n_1 の倍数かつ n_2 の倍数で、

$$x_2 \equiv x_1 \pmod{n_1} \quad \text{かつ} \quad x_2 \equiv x_1 \pmod{n_2}$$

つまり

$$x_2 \equiv A_1 \pmod{n_1} \quad \text{かつ} \quad x_2 \equiv A_2 \pmod{n_2}$$

である。

これを繰り返して

$$x_e \equiv A_i \pmod{n_i}, \quad (i = 1, 2, \ldots, e)$$

となる整数x_eで$0 \leq x_e < n_1 n_2 \cdots n_e$を満たすものを求めることができる。

$A^e - x_e$は各$n_1, n_2, \ldots, n_e$で割り切れるのでそれらの積$n_1 n_2 \cdots n_e$で割り切れるが、Aもx_eも$n_1 n_2 \cdots n_e$より小さいので、$A^e = x_e$である。すなわち$A = \sqrt[e]{x_e}$として求まる。

以上で必要な操作はユークリッドの互除法とe乗根を求めるだけで、n_iの素因数分解は必要ないので、この計算は実用的な時間内に行うことができる。

本講に関するより詳しい内容は [長嶋 福田] 参照のこと。

参考文献

[新居] 新居俊作 著
「コンピュータの基礎理論」
https://www2.math.kyushu-u.ac.jp/~snii/computer.pdf

[Shor] P.W. Shor
"Algorithms for quantum computation: discrete logarithms and factoring"
Proceedings 35th Annual Symposium on Foundations of Computer Science (1994). IEEE Comput. Soc. Press: 124–134.
doi:10.1109/sfcs.1994.365700. ISBN 0818665807.

[長嶋 福田] 長嶋 祐二 福田 一帆 共著
「基礎から学ぶ整数論 RSA 暗号入門」
コロナ社 2020 年