基礎から学ぶ整数論

── RSA 暗号入門 ──

博士(工学) 長嶋　祐二
博士(工学) 福田　一帆
【共著】

コ ロ ナ 社

ま　え　が　き

私たちの生活でなじみ深い自然数という数(かず)は，ヒトの誕生そして進化する過程の中で，ものを数えるという行為や，順序・順番というと考え方とともに発生し，徐々に概念形成が行われたと考えられます。私たち漢字圏の生活の中では，一（1），十（10），百（10^2），千（10^3），万（10^4），億（10^8），兆（10^{12}），$\cdots$の漢数字が用いられています。知られている最大数は，恒河沙(こうがしゃ)（10^{52}），阿僧祇(あそうぎ)（10^{56}），那由他(なゆた)（10^{60}），不可思議(ふかしぎ)（10^{64}），無量大数(むりょうたいすう)（10^{68}）のほか諸説ありますが，無量大数です。この数(かず)という概念形成の過程で，数(すう)という抽象概念へと発展していたと考えられます。では，位取りには欠かせない 0 は，いつから使われるようになったのでしょうか。ゼロ「0」はインドで使われだしたというのが有力な説です。この 0 の発見により数学が爆発的に進歩したともいわれています。そして，0 が，整数論の体系化に大きく寄与した記号と考えられます。

整数論の中で，その不思議さ・難しさ・神秘さがゆえに私たちを魅了し続けている数(かず)に 6 章で学ぶ素数があります。素数は，すでに古代ギリシャの数学者ユークリッドにより，無限個の存在が証明されています。さらに，素数を効率的に見つける方法は，古代ギリシャの数学者 エラトステネスが考案したとされる「エラトステネスの篩(ふるい)」です。そして，素数の出現には規則性がないとされているため，いまだにエラトステネスの篩を上回る素数を見つける方法はないとされています。この素数が，現代の高度情報化社会の情報通信の安全性を根底から支える暗号に用いられています。インターネット上の情報は，暗号化することで安全に通信相手に送ることができるようになります。さまざまな暗号技術が考案されていますが，実用化されている暗号技術の中に，大きな二つの異なる素数を用いる RSA 暗号があります。残念ながら，RSA 暗号は未来永劫に安全な暗号技術とはいえません。いままさに新しい暗号技術の研究が進んで

います。しかし，安心してください，まだ RSA 暗号は安全とされています。

本書は，中学生レベルの整数の知識を基に整数論の基礎を理解しながら，RSA 暗号の基礎となる考え方を学ぼうとする読者を想定してまとめてあります。数学科ではない学生は，整数の話題に興味はあるが難しいと感じている人も多いと思います。そのような人は，暗号に興味があるけれど，なにから始めてどのように学んだらよいかわからないと思います。学生ではなくても，RSA 暗号を学びたいのになにから始めたらよいかわからない人も多くいると思います。RSA 暗号を学ぶのにいきなり，合同式や素数に関する難しい定理や素数に関する難解な演算からスタートするのは避けたいものです。

本書で RSA 暗号を学び始めるために最低限必要な数学の知識は，中学生までに学んだ整数の四則演算だけです。はじめに，1 章において RSA 暗号の概要を学び，目的を明確にします。ここでは，RSA 暗号の仕組みや特徴を学び，「なぜそのようなことが可能なのか」という疑問をもつことが大切です。読者の皆さんは，1 章を終えた時点で，RSA 暗号について理解できない部分があっても，まったく問題ありません。つぎに，2 章から 6 章では，RSA 暗号の理解に必要な整数論の各項目を学びます。ここでは，中学高校レベルの知識から始まり，徐々に新しい定理や知識を身に付けていきます。各項目と RSA 暗号との関係は，目次の $\star$ の数で表してありますので，参考にしてください。RSA 暗号の計算をできるようになるためには $\star\star$ まで，RSA 暗号の原理を理解したい場合は $\star\star\star$ までの知識が必要となります。最後の 7 章では，再び RSA 暗号に戻り原理の理解と実践を目指します。6 章までを修得していれば，1 章では疑問だらけだった RSA 暗号が，7 章ではスラスラと計算でき原理も理解できるようになるはずです。

整数論と RSA 暗号を学ぶためには，さまざまな定理を理解しなければなりません。重要あるいは必要な定理には，詳細な証明を載せるように心がけました。そして，それらの定理の使い方を学ぶために例題を用意してあります。例題には，わかりやすい解答過程を載せるようにしました。また，各章の章末には章全体の理解確認の問題を用意してあります。各章末問題の解答は，なるべ

く詳細に計算過程を載せるように心がけました。さらに，基本的な計算過程のほかに理解を補う別解法がある場合には，その過程も載せるようにしています。

本書の例題や章末問題などは，数式処理言語である Mathematica を用いて計算することができます。興味のある人は，Mathematica にも挑戦してみてください。

なお，本書は工学院大学情報学部の 1 年生共通科目として設置している情報数学および演習 3 の教科書としてまとめたものです。「情報数学および演習 3」は講義と演習の 2 限連続 × 全 7 週のクォーター科目であり，本書は全 14 コマで扱う内容となっています。情報学部情報デザイン学科の設立のとき，基礎科目に整数論や暗号に関する授業がありませんでした。そこで，2009 年に整数論の講義を開始し，2013 年には RSA 暗号を追加しました。そして，2016 年から情報学部全体の 1 年生基礎科目として，整数論の基礎と RSA 暗号を学ぶ情報数学 3 が開始されました。これに伴い，TEX の jarticle 形式から jbook 形式に授業資料の充実を目指して再構築を開始しました。2019 年には，充実化が終了したので出版準備に取り掛かりました。本書の校正にご協力をいただいた本学の非常勤講師の渡邉桂子先生には，わかりにくいところなどいろいろご意見をいただいたことに感謝いたします。

最後に，出版を快諾していただくとともにさまざまなコメントをいただいたコロナ社の皆さまに感謝いたします。

追記：2019 年末ごろより，人知れず人への感染力を獲得してしまった「新型コロナウイルス（SARS coronavirus 2（SARS-CoV-2））」が中国の武漢市を中心に出現しました。この新型コロナウイルス感染症（coronavirus disease（COVID-19））の患者数が，世界中で爆発的に増加しており，日本でもその増加の脅威が拡大しております。1 日も早いこの感染症の終息を願い執筆を終了しました。そして，出版時には終息していることを願うばかりです。

2020 年 8 月

長嶋 祐二
福田 一帆

凡　　例

(1) 本書は，7 章で構成されています。自分の理解している章は飛ばしてつぎの章から読んでも大丈夫です。また，必要な章のみを読むことができるようになっています。

(2) 内容理解のために，例題，章末問題を用意しています。すべての問題には詳細な解答を付けています。また，別な解法があるときには，なるべく別解も詳細に記載するようにしています。

(3) 重要と思われる用語には，その対応英語も付けています。

(4) 目次の各項目には本書を読んで，どこまでの知識を得られるか（重要度）を ⋆ の数で示してあります。

無印	：	事前知識，参考
⋆	：	高校までの復習程度の知識
⋆⋆	：	RSA 暗号の計算に必要な知識
⋆⋆⋆	：	RSA 暗号の原理の理解に必要な知識

(5) 本書において，計算過程や変形過程の項や数字，表中の数字に付した ____，＝＝＝＝，～～～，..... は，同じ種類のラインとの対応関係に注目してもらいたい部分です。また，重要な概念にも ～～～～ を付してあります。

(6) 数学の用語としてよく見かける公理と本書で用いている用語について説明します。

(a) 公理（axiom）　その理論の出発点であり，証明をしないで用いることのできる記述（文章や式）のことです。その議論の出発点となる最も自明な前提条件とも考えられます。したがって，証明する必要がないのです。ユークリッド幾何学に出てくる「平行線の公理」は有名です。

(b) 定義（definition）　本書において，用語の意味や式を定めたもので，証明をしないで用いている議論の前提条件です。具体的な例は，本文を参照してください。

(c) 定理（theorem）　本書において，定義から導出することのできる記述（文章や式など）を指します。公理や定義，そして証明済みの

定理を用いて証明することができます。具体的な例は，本文を参照してください。

(d) 補題（lemma）　本書では，定理から類推，あるいは導出することができる記述（文章や式など）を指します。定理と同様に証明することができます。具体的な例は，本文を参照してください。

(e) アルゴリズム（algorithm）　本書では，問題を解く手順が規則化されていて，プログラム化することで容易に解を求めることができる手法の記述に用いています。アルゴリズムの記述方法は，プログラミング言語を特定しないように，代入式，判断式，計算式などを用いて記述しています。具体的な例は，本文を参照してください。

(f) 参考（guide）　本書では，直前の記述や例題などに対して，考え方や計算の手助けとなる記述や式を参考として記述しています。具体的な例は，本文を参照してください。

(g) 例題（example）　本書では，直前の内容の確認のため，あるいはつぎの項目の準備として必要な知識の確認のために，多くの例題を記載しています。確認のためにあるので，定義・定理・アルゴリズムの文の直後に記載してあります。

(7) 本書の 4 桁以上の数値の表記では，3 桁ごとの区切り記号としてカンマ「,」ではなく空白を用います。小数点にはピリオド「.」を用います。例えば，123456789 は 123 456 789 と表記しています。この区切り記号や小数点記号になにを用いるかは国によっても異なります。

注 1）本文中に記載している会社名，製品名は，それぞれ各社の商標または登録商標です。
注 2）本書に記載の情報，ソフトウェア，URL は 2020 年 4 月現在のものを掲載しています。

本書で用いるおもな記号とその意味

本書で用いているおもな記号とその意味について挙げます。なお本書において，乗算では，掛けることを意識的に示したり，わかりやすさのために，$a \times b$，$a \cdot b$，$3 \times a$ のように演算子 $\times$ や $\cdot$ を適宜用います。省略してもわかるときには，ab や $3a$ のように表記します。また，$n_1 n_2 \cdots n_{10}$ や $n_1 + n_2 + \cdots + n_{10}$ などの $\cdots$ は，積や和の繰り返し演算を示しています。

自然数全体の集合　：$\mathbb{N}$，　$\mathbf{N}$（Natural number）

整数全体の集合　：$\mathbb{Z}$，　$\mathbf{Z}$（Integral number ドイツ語　数 Zahl）

有理数全体の集合　：$\mathbb{Q}$，　$\mathbf{Q}$（Rational number，ドイツ語　商 Quotient）

実数全体の集合　：$\mathbb{R}$，　$\mathbf{R}$（Real number）

複素数全体の集合　：$\mathbb{C}$，　$\mathbf{C}$（Complex number）

$b \mid a$　：a は b で割り切れる，$\dfrac{a}{b}$ が整数の商 q をもつ。

$a = b \times q$（$b \neq 0$）

$b \nmid a$　：a は b で割り切れない，$\dfrac{a}{b}$ が整数の商をもたない。

$\mathrm{GCD}(a, b) = (a, b)$　：a と b の最大公約数

$\mathrm{LCM}(a, b) = [a, b]$　：a と b の最小公倍数

$\lfloor x \rfloor =$　：床関数，x を超えない最大の整数

$\max\{n \in \mathbb{Z} | n \leqq x\}$　　例）$\lfloor 3.14 \rfloor = 3$，$\lfloor -3.14 \rfloor = -4$

$[x]$　：ガウス記号，x を超えない最大の整数，床関数と同じ

$\lceil x \rceil =$　：天井関数，x 以上の最小の整数

$\min\{n \in \mathbb{Z} | x \leqq n\}$　　例）$\lceil 3.14 \rceil = 4$，$\lceil -3.14 \rceil = -3$

$a \equiv b \pmod{n}$　：a と b は n を法（modulus）として互いに合同である。

「a を n で割った余り」＝「b を n で割った余り」

⇕ 同じ意味

$n \mid a - b$

$x \in \mathbb{Z}$　：x は $\mathbb{Z}$ に属する，x は集合 $\mathbb{Z}$ の元である。

$\forall$　：全称記号で，$\forall x$ は「任意の x」，「すべての x」を表す。

$\exists$　：存在記号で，$\exists x$ は「ある x が存在して」を表す。

$\prod$　：総乗（product）記号

例）$\displaystyle\prod_{i=1}^{n} x_i = x_1 x_2 \cdots x_n$

$\simeq$　：$\fallingdotseq$ と同じ意味

$\leqq$　：$\leq$，$\leqslant$ と同じ意味

$\geqq$　：$\geq$，$\geqslant$ と同じ意味

$\ll$　：十分小さい

$\gg$　：十分大きい

$\vee$　：論理和，または

$\wedge$　：論理積，かつ

$\cup$　：和集合，$A \cup B$ は A または B の要素からなる集合

また，C_1から C_nまでの n 個の集合の和集合を

$C_1 \cup C_2 \cup C_3 \cup \cdots \cup C_n = \displaystyle\bigcup_{r=1}^{n} C_r$ と表す。

$\cap$　：積集合，$A \cap B$ は A と B の共通部分の集合

また，C_1から C_nまでの n 個の集合の積集合を

$C_1 \cap C_2 \cap C_3 \cap \cdots \cap C_n = \displaystyle\bigcap_{r=1}^{n} C_r$ と表す。

$\therefore$　：ゆえに

$\because$　：なぜならば，なんとならば

$i.e.$　：すなわち，*idest*（ラテン語：イデェストゥ）の省略形

$A \subset B$：A は B の真部分集合，「A は B に含まれ」かつ「$A \neq B$」

$A \subsetneqq B$ あるいは $A \subsetneq B$ とも書く。

$A \subseteq B$：A は B の部分集合，$A \subseteqq B$ とも書く。

$\binom{n}{r}$　：2 項係数，${}_nC_r$ と同じ

目　　次

1. 整数の基礎的知識 ── RSA 暗号の導入 ──

2. 最小公倍数と最大公約数 ── 整数の組に共通性を探す ──

3. ユークリッドの互除法 ── 最大公約数を効率的に求める ──

4. 一次不定方程式 ── RSA 暗号の理解の手助け ──

5. 合同式 ── RSA 暗号の暗号鍵の計算に必要 ──

6. 素数 ── RSA 暗号を根底から支える数 ──

7. RSA 暗号 ── さぁ RSA 暗号に挑戦 ──

定義，定理，アルゴリズム一覧

1 整数の基礎的知識 ── RSA 暗号の導入 ──

本書では，RSA 暗号（RSA encryption）の原理の理解を目標とします。RSA 暗号を求めるのに必要となる，さまざまな基礎的な整数論の定理，演算手法を学びます。

1 章では，暗号の基礎知識と RSA 暗号の導入，数と式について学びます。本章の後半 1.5 節からは，中学校から高等学校までの整数の知識の復習です。

1.1 RSA 暗号の導入

暗号（cryptography）とは

> 送信者が，伝えたい大事な情報（メッセージ）を第三者には内容が知られないように（秘匿）し，正規の受信者だけが解読できるようにする秘匿通信の手段

のことである。ここで，元のメッセージを**平文**（ひらぶん）（plaintext），第三者に秘匿する形にしたメッセージを**暗号文**（cryptogram），平文を暗号文に変換する過程を**暗号化**（encryption），その逆の暗号文を平文に変換する過程を**復号**（decryption）という。

優れた暗号の条件は

- 当事者以外の第三者に解読が困難
- 汎用性が高い（一つの方法でさまざまな情報に使える）

である。

1.2 暗 号 の 歴 史

最古の暗号は，紀元前 3000 年ごろと推定される古代エジプトで用いられていた象形文字であるヒエログリフといわれている。ヒエログリフの解読のきっかけは，1799 年 7 月に発見された「ロゼッタストーン」と呼ばれる石碑である。

紀元前 6 世紀ごろには，古代ギリシャの都市国家のスパルタでは，「**スキュタレー暗号**」が使用されていた。このスキュタレー暗号の「スキュタレー」とは，暗号文を作る際に用いられた太さの一様な棒のことである。送信者は革ひもを棒に沿って巻き，棒に沿って文字を書く。革ひもを受け取った受信者は，送信者が使った棒と同一な直径の棒に革ひもを巻き付けると解読できる。この暗号では，棒の直径が鍵となる。

古代の暗号で最も有名なのが，紀元前 1 世紀ごろの古代ローマで Julius Caesar（古典ラテン語ではユリウス カエサル，英語読みではジュリアス シーザー）が使ったとされる「**シーザー暗号**」である。暗号文は，元の文章のアルファベットをあらかじめ決められた文字数だけずらして暗号文を作成する。この何文字ずらすかが暗号鍵となる。この方式の暗号化法を**換字式暗号方式**（かえじ）と呼ぶ。例えば，3 文字ずらす場合，A → D, B → E, C → F, ⋯, W → Z, X → A, Y → B, Z → C という変換を行う。送りたい文章の平文：DOG では，暗号文：GRJ となる。

1.3 共 通 鍵 暗 号

1.3.1 共通鍵暗号とは

データの暗号化と復号に同じ鍵を使う暗号方式のことで，**秘密鍵暗号**（secret key cryptography）ともいう。共通鍵は一般的に暗号の送信者が作成し，暗号文とともに，または別の手段を用いて受信者に送信する。共通鍵暗号の概念を**図 1.1** に示す。

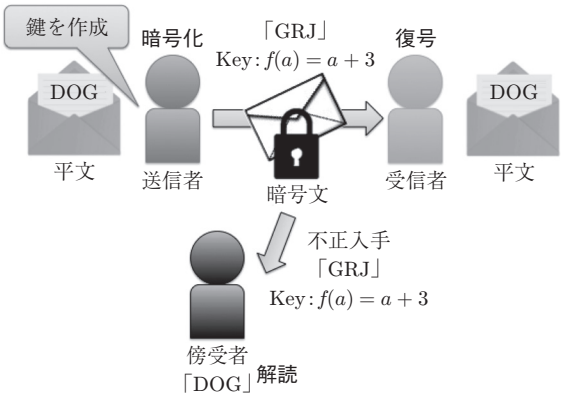

図 1.1 共通鍵暗号の概念図

1.3.2 共通鍵暗号の弱点とその対策

共通鍵暗号（common key cryptography）では，共通鍵が盗まれると暗号が解読されてしまう。そのため，どのように安全な方法で相手へ秘密の鍵を伝えるかが問題である。また，送信相手が多くなるほど危険性も高まる。その弱点の対策として考えられたのが，「鍵を送らなくてよい」公開鍵暗号である。

1.4 公 開 鍵 暗 号

1.4.1 公開鍵暗号とは

公開鍵暗号（public key cryptography）とは，ペアとなる二つの鍵を用いて，データの暗号化と復号を行う暗号方式のことである。この方式では，鍵は一般的に暗号の受信者が作成する。受信者は**暗号化鍵**と**復号鍵**のペアを作成して，復号鍵を厳重に管理する（そのため，復号鍵は**秘密鍵**とも呼ばれる）。そして，もう一方の暗号化鍵は広く他人に公開する（そのため，**公開鍵**とも呼ばれる）。この公開鍵で暗号化されたデータはペアとなる秘密鍵でしか復号できない。この方式では，復号鍵を送受信する必要がないため安全性が高い。公開鍵暗号の概念を**図 1.2** に示す。

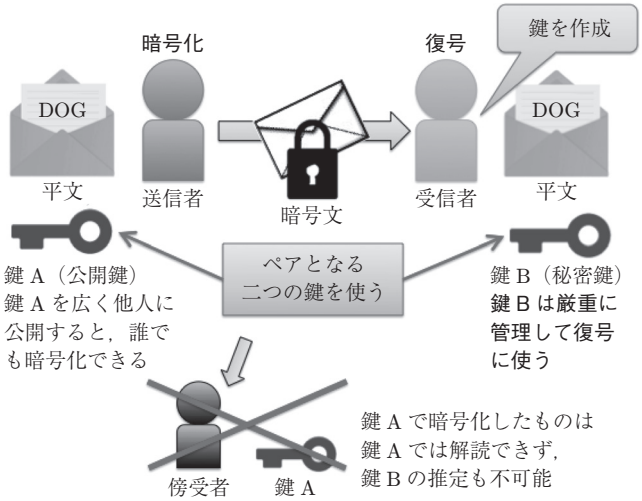

図 1.2　公開鍵暗号の概念図

1.4.2 原　　理

公開鍵暗号において，暗号化鍵，復号鍵，平文，暗号文との関係を**図 1.3** に示す。

公開鍵暗号の原理

・暗号化鍵（公開鍵）	$\neq$	復号鍵（秘密鍵）
・平文 $\otimes$ 公開鍵	$=$	暗号文
・暗号文 $\otimes$ 公開鍵	$\neq$	平文
・暗号化鍵（公開鍵）	から	復号鍵（秘密鍵）の推定が困難
・暗号文 $\otimes$ 秘密鍵	$=$	平文

ただし，$\otimes$ は暗号化や復号過程の演算子を表すものとする。

図 1.3　公開鍵暗号の原理

1.4.3 RSA　暗　号

RSA 暗号は，1977 年に MIT（マサチューセッツ工科大学）の Ronald L. Rivest, Adi Shamir, Leonald Adleman により発明された。RSA 暗号は，最

も古くからある，最も有名な公開鍵暗号である。その信頼性は，大きな素数の**素因数分解**（prime factorization）の困難さに基づいている。

表 1.1 に示す RSA 暗号の手順は，鍵を生成する過程，平文からの RSA 暗号化して暗号文を求める過程，そして，暗号文を解読して元の平文を求める過程の (1) から (5) となる。表 1.1 の (1) から (5) の意味や計算方法は，次章から詳細に解説を行う。そして，最終章の 7 章では，RSA 暗号の原理とその実際の処理手順を学ぶ。

表 1.1 RSA 暗号の手順と必要な知識

RSA 暗号の手順	必要な知識
(1) $n = p \times q$　ただし，p, q は相異なる奇素数	素数（6.1 節）
(2) $\mathrm{GCD}(e, \varphi(n)) = (e, \varphi(n)) = 1$ となる e を求める	オイラーの関数（6.2 節）
(3) $ed \equiv 1 \pmod{\varphi(n)}$ を満たす d を求める n, e を公開鍵，d を秘密鍵とする	一次合同式の解法（5.5.5 項）
(4) $A \xrightarrow{\text{暗号化}} A'$，$A' \equiv A^e \pmod n$ (5) $A' \xrightarrow{\text{復号}} A$，$A \equiv (A')^d \pmod n$ } $A^{ed} \equiv A \pmod n$ ただし，A : 平文，A' : 暗号文	フェルマーの小定理（6.3.1 項） ◊なぜ，$A^{ed} \equiv A \pmod n$ が成立する？ $\Longrightarrow$ 定理 6.14（6.3.2 項）

注） 奇素数 : 2 以外の素数

表 1.1 において，n, e が暗号化鍵となり，公開してもよいので公開鍵となる。また，p, q, e から求まる d が復号鍵となり，秘密にしておくので秘密鍵となる。なお，表 1.1 は，6 章の「RSA 暗号の手順のまとめ」に掲載の表 6.1 と同じである。

1.5 数 と 式

1.5.1 自 然 数

日常使われる数というのは物の数 $1, 2, 3, \cdots$ であり，**計量数**または**集合数**（cardinal number）である。また数は順序 $1, 2, 3, \cdots$ を示す**順序数**（ordinal

索　　引

—— 著 者 略 歴 ——

長嶋　祐二（ながしま　ゆうじ）
1978年　工学院大学工学部電子工学科卒業
1980年　工学院大学大学院工学研究科修士課程修了（電気工学専攻）
1980年　工学院大学助手
1989年　工学院大学講師
1993年　博士（工学）工学院大学
1994年　工学院大学助教授
2003年　工学院大学教授
　　現在に至る

福田　一帆（ふくだ　かずほ）
2001年　千葉大学工学部画像工学科卒業
2003年　東京工業大学大学院総合理工学研究科修士課程修了（物理情報システム専攻）
2006年　東京工業大学大学院総合理工学研究科博士課程修了（物理情報システム専攻）博士（工学）
2006年　東京工業大学産学官連携研究員
2006年　York 大学（カナダ）博士研究員
2009年　東京工業大学特任助教
2010年　東京工業大学助教
2014年　工学院大学准教授
　　現在に至る

基礎から学ぶ整数論　—RSA 暗号入門—

Fundamentals of Number Theory —Introduction to RSA Encryption—

2020 年 10 月 8 日　初版第 1 刷発行　★

検印省略

著　者　長嶋　祐二
　　福田　一帆
発行者　株式会社　コロナ社
　　代表者　牛来真也
印刷所　三美印刷株式会社
製本所　有限会社　愛千製本所

112–0011　東京都文京区千石 4–46–10
発行所　株式会社　**コロナ社**
CORONA PUBLISHING CO., LTD.
Tokyo Japan
振替 00140–8–14844・電話(03)3941–3131(代)
ホームページ　https://www.coronasha.co.jp

ISBN 978–4–339–06120–8　C3041　Printed in Japan　（松岡）