特集「数論アルゴリズムとその応用」の編集にあたって

岡　本　龍　明†

数学の諸分野の中でも，数論（整数論）は，実用的応用（物理等への応用も含めて）のない純粋理論の最右翼と考えられていた．ところが，最近の暗号理論や符号理論では，この数論が重要な手段として使われるようになってきており，さらに，初等的な数論の枠を越えた理論にまで応用の範囲を広げつつある．例えば，最近の暗号理論や符号理論を学ぶには，初等整数論や有限体の理論の知識が必要であり，また，代数的整数論や代数曲線論などと関連する暗号や符号理論の研究も盛んに行われている．

それでは，従来役に立たない数学理論の代表であった数論が，なぜこのように応用されるようになってきたのであろうか？　それは，現在のコンピュータやネットワークの多くが，2値（0, 1）に基づくディジタル情報（離散情報）を基本に構成されており，一方，数学の中でこのような離散情報を自然に扱うことのできる理論の代表が数論であるからであろう．つまり，暗号や符号への応用において，0, 1で表現されたディジタル情報は，2進数表現を媒介として整数や有限体の要素に対応づけられるわけである．一旦，整数や有限体の世界に翻訳された情報は，その数の世界での理論に応じた処理が可能となる．このとき，これらの数の世界に関する数学理論が利用されるが，その一方で，従来の数学者があまり興味を持たなかった効率的なアルゴリズムといった問題については，新たな研究課題が山積していることになる．

今回の特集では，このように，暗号や符号への応用に刺激されて，1970年代後半以降に急速に発展した，数論に関するアルゴリズムとその応用について解説を行うものである．

さて，それでは，この数論アルゴリズムとは，どのようなアルゴリズムのことを呼ぶのだろうか？　最近，この分野の第一人者である Erich Bach が，数論アルゴリズム全般を紹介する論文を表しているが[1]，参考までにその目次を紹介しよう．これにより，現在主に研究されている数論アルゴリズムの概要を知ることができる．1. 数学的基礎知識（計算理論，代数，素数定理，リーマン予想，代数幾何，確率論），2. 基本アルゴリズム（剰余演算，ユークリッドの互除法，一次方程式），3. 有限体上のアルゴリズム（平方根，多項式の因数分解，楕円曲線，乱数性），4. 素数判定（フェルマーの定理に基づく判定，各種アルゴリズム），5. 素因数分解（計算量の評価，各種アルゴリズム，素因数分解と関連する暗号学的問題），6. 離散対数問題（一般的算法，準指数的算法）．

本特集では，数論アルゴリズムとして，素数判定，素因数分解，離散対数問題，有限体上のアルゴリズム，多倍長・高速剰余演算，代数幾何学的アルゴリズムを取り上げた．さらに，本特集では，この数論アルゴリズムが，符号理論及び暗号理論でどのように応用されているかを紹介する．

以下に各解説の紹介を行う．

1.「数論アルゴリズムの研究動向」

本特集の導入として，本解説では，数論の基礎的知識，及び数論アルゴリズムの概要について入門的解説を行う．特に，これに続く2.「素数判定アルゴリズム」及び3.「素因数分解と離散対数問題アルゴリズム」の導入ともなっているため，これらの解説を読まれる際には，是非本解説を最初に読まれるようお奨めする．

2.「素数判定アルゴリズム」

ある整数が与えられたとき，それが素数であるかどうかを判定するアルゴリズムが素数判定アルゴリズムである．本解説では，この素数判定に関する各種アルゴリズムの解説を行う．素数判定アルゴリズムの研究においては，（1）実際にプログラムを作って，指名手配のある大きな数が実際に素数であることを証明するような具体的アプローチと，（2）素数判定問題がどの計算量のクラスに属するのかを調べるような計算量理論的アプローチの二つの立場がある．本解説では，この両方の立場からの解説が行われている．つまり，前者の立場からは，研究者により作られた素数判定プログラムの入手方法も含めて，アルゴリズムの解説が行われ，後者の立場からは，アルゴリズムの厳密な計算量の評価が述べられている．

3.「素因数分解と離散対数問題アルゴリズム」

公開鍵暗号を構成するには，解くのが難しい（と思われている）問題が利用されるが，その代表例が，「素因数分解」と「離散対数問題」である．素因数分解問題は，合成数が与えられたとき，それを素因数に分解する問題であり，離散対数問題は，有限群（有限個の元から構成される群）上の対数問題（(g, g^x) から x を求める問題）である．本解説では，楕円曲線法や数体ふるい法といった最新のアルゴリズムを中心に，現在までに提案されている代表的なアルゴリズムの解説を行う．さらに，数値実験結果や計算量理論，暗号理論との関連についても論じている．

† NTT 情報通信網研究所

4.「有限体上のアルゴリズムと多倍長・剰余演算の高速演算法」

多くの符号や暗号は，有限体の演算に基づいて構成される．また，剰余演算に基づく有限環上で構成される暗号系も多い．このような，符号系や暗号系においては，それら有限体や有限環上の各種演算を効率的に行うことが要求される．また，素数判定や素因数分解，離散対数をはじめとする数論アルゴリズムでは，数100桁以上の大きな数を扱うことが多くあり，そのような大きな数を扱うアルゴリズム（多倍長演算）が必要である．本解説では，有限体上の四則演算，多項式の素因数分解の効率的アルゴリズムの解説を行う．また，多倍長演算アルゴリズム，及び，有限体や有限環における剰余演算を高速に実現する各種アルゴリズムを解説する．なお，本解説と密接に関連する解説として，森田氏の「暗号技術と高速算法」が次号（93年3月号）に掲載される予定であるので，あわせてご一読いただきたい．

5.「代数幾何学的アルゴリズム」

1980年代に入って，代数曲線（楕円曲線を含む）を用いた符号理論，暗号理論，素因数分解アルゴリズム，素数判定アルゴリズム等が知られるようになった．本解説では，このような各種応用において，基本となる代数曲線上のアルゴリズムについて解説を行う．具体的には，有限体上の楕円曲線の元の数を計算するアルゴリズムやその群構造を計算するアルゴリズム，及び一般の代数曲線上の Riemann-Roch の定理に関するアルゴリズム等について解説を行う．

6.「符号理論への応用」

本解説では，数論アルゴリズムを用いて，いかに符号系が構成されるかについて解説を行う．従来より，符号理論は有限体の理論を基に構築されてきたが，特にここでは，最近の研究の進展の著しい代数曲線上の符号（代数幾何符号）について説明を行う．代数幾何符号は，BCH 符号など従来主に研究されてきたほとんどの符号を含む広範な符号体系を構築するものであり，さらに，この体系の中で従来の限界を破る新しい符号が構成できるようになった．まず，符号化がどのように行われるかについて説明を行い，次に，基本的な復号化のアルゴリズムを説明する．

7.「暗号理論への応用」

本解説では，数論アルゴリズムを用いて，いかに暗号系が構成されるかについて解説を行う．まず，素因数分解もしくは離散対数問題を利用したいくつかの代表的な公開鍵暗号とディジタル署名法の解説を行う．引き続き，離散対数問題を用いた疑似乱数生成器の構成法について述べる．なお，この疑似乱数生成器の安全性が，基本となる離散対数問題の困難性と等価であることの証明も示される．最後に，有限体上での楕円曲線を用いた公開鍵暗号の構成法について解説を行う．本解説の前半に紹介した離散対数問題を用いた公開鍵暗号を基にして，楕円曲線暗号がどのように構成されるかを解説する．

ところで，実際に数論アルゴリズムのプログラムを書く場合に，まず直面する問題が，大きな整数を扱うための処理である．これについては，本特集の中でも 4.「有限体上のアルゴリズムと多倍長・剰余演算の高速演算法」で，扱われているが，このような処理を自作しないで，簡単にプログラムを書きたいとお考えの方には，市販のいわゆる数式処理用のツールを利用することをお勧めしたい．このようなツールを使うと，大きな整数の演算のプログラムを容易に書けるだけでなく，さらに，素数判定や素因数分解，各種演算サブルーチン等のプログラムが標準関数として提供されている場合も多い．（但し，最新の高速なアルゴリズムが用いられているとは限らないので，マニュアルで，使用されているアルゴリズムを確認されたい）．このようなツールとしては，例えば Macsyma, Mathematica, Maple, muMATH, REDUCE 等[2] があり，さらに，本特集の著者の一人でもある木田氏作成のU-Basic は，特に数論関連の機能に優れた特徴がある．

この分野の研究が活発に行われるようになったのが比較的最近であるためか，これまで，本特集で紹介したような数論アルゴリズム全般に関する成書はもとより，解説記事も無かったようである．本特集が，数論に関するアルゴリズムのプログラムを利用，作成される方，また，数論アルゴリズムに興味を持たれて勉強をしてみようと思っている方々のお役に立てば幸いである．

ご多忙にもかかわらず，執筆を快諾し多大な時間をさいていただいた執筆者の方々，ならびに編集，閲読にご協力いただいた方々に深く感謝いたします．

参考文献

1) Bach, E. Number-Theoretic Algorithms, Ann. Rev. Computer Science, 4, pp. 119-172 (1990).
2) Foster, K. R. Prepackaged math, IEEE SPECTRUM, November, pp. 44-50 (1991).

（平成4年12月22日）