小特集

素　数

小特集編集にあたって

編集チームリーダー　趙　晋輝

数学の工学への応用といえば，恐らく最も有名なのは公開鍵暗号である．1970 年代彗星のごとく現れた RSA 暗号は，二つの大きな素数同士の掛け算は簡単であるが，その積から素因数を求めるのは難しい，という一方向性を巧妙に利用した方式であり，現在でも最も分かりやすく，使いやすく，しかも美しい暗号の一つとして活躍している．

「数を神が作った」といわれるほど，本来の整数論はピタゴラス時代から，神秘の対象ともされてきた．整数論が数学の女王といわれる理由も，それが数学のほかの分野の知見や手法を駆使することがあっても，他人のために役立った試しは一向にないことから，そのように言われている．このような孤高な整数論も，今日では万人が日ごろ使うようになっているインターネットや電子機器などに応用され，社会の基本インフラを担っていることは，まさに驚嘆に値する．

また，暗号という極めて実学的な学問に対して，強い関心を寄せ，暖かく見守って頂いている純粋数学者が数多くおられることも，誠に有り難い．今回，整数論の不思議な魅力について，九大の金子昌信先生が工学者向けに素晴らしい解説を書いて下さった．名文に感銘するとともに，御多忙極まる中で御執筆を快諾頂いた金子先生に感謝申し上げる．

整数論は暗号の理論と道具を提供しているだけではなく，コンピュータサイエンスの基礎理論や計算アルゴリズムに対して，新しい問題，発想として手法を与え続けてきた汲めども尽きぬ泉でもある．近年，長年未解決の「素数判定は確定的多項式時間クラスに属するか」という問題がついに解決され，コンピュータサイエンス界の久しぶりのビッグニュースとなった．これに関連して，首都大東京の内山成憲先生が大変興味深い対談を書いて下さった．

さて，日本の整数論は，世界の最高水準であることがよく知られている．一方で，日本の暗号研究も世界のトップレベルを誇っている．昨今話題となっているのは，NTT 青木和麻呂さんの国際的グループが最近樹立した素因数分解の新しい世界記録と下山武司さんをはじめとする富士通研の研究者らが開発した素因数分解用の専用ハードウェアである．現時点で RSA に使われている合成数の標準鍵長は 1,024 ビットであるが，この新世界記録は，特殊な形とはいえ，1,017 ビットの合成数を素因数分解する大変衝撃的なものである．

更に，暗号系に対して現時点で知られている攻撃の中で潜在的に最も強力といわれているのは，専用ハードウェアによるものである．しかし，理論的な見積もりがほとんどで，確かな検証が行われていない．下山さんたちの努力によってあるレベルまでその疑問に確実に答えたのである．この二つの話題についてはそれぞれ青木さんと下山さんに大変迫力のある記事を書いて頂いた．

また，RSA 暗号が提案されてから暗号研究者を悩ませ続けた問題がもう一つある．それは，素因数分解ができれば RSA 暗号は解けるが，逆に素因数分解をうまく避けるように RSA 暗号を解読できるか，という問題である．この問題については，東大の國廣昇先生に「素因数分解は RSA 暗号解読より真に難しいか？」の記事で，最新の進展について大変分かりやすく紹介して頂いた．

短期間内で御多忙極まるにもかかわらず御協力を頂いた執筆者の皆様には深く御礼申し上げたい．また，理工離れの今日に，純粋にこのテーマに興味を持つ方が一人でも多くなることを願っている．