＜コラム：数学の女王 整数論＞

これまでの数学では、さまざまな「数」について学んできた。その中でも、物の値段や温度、日付や時間など身の回りに多く存在する数は、1 や 0、-3 などの整数だろう。

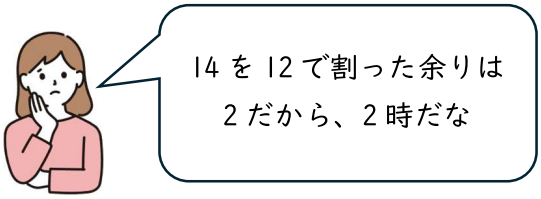
ヨハン・カール・フリードリヒ・ガウス(1777-1855 年)という有名なドイツの数学者・物理学者は、整数を探究する数学の分野である「整数論」を、**数学の女王**とよんだ。(正確には、「数学は科学の女王であり、数論(整数論)は数学の女王である」といった。)

ガウスが整数論を数学の女王とよんだのは、整数論が美しい理論であるからである。また、後世の数学者には、整数論は美しいだけで、実生活や他分野の役に立たないからこそ、ガウスは「王」ではなく「女王」であると言い残したのだと考える者もいた。

では、実際に整数論は身の回りの役に立たないのだろうか？少し考えてみよう。

整数論の主役ともいえるのが、**素数**である。素数は 2,3,5,7,…と続く、1 とその数自身でしか割り切れない 2 以上の整数である。多くの人が素因数分解で学んだように、すべての整数は素数の掛け算で表すことができる。(例：12 = 2 × 2 × 3) 素数にまつわる問題は、いくつも存在する。例えば、「素数は無限に存在するのか？」という問題は、古代ギリシャの数学者であるユークリッドにより、「無限に存在する」という答えが出されている。他にも、「素数の出現には規則があるのか？」という問題もある。この問題はかの有名な「リーマン予想」にも関係しており、160 年以上もの間、世界中の天才数学者たちが挑戦しているものの、未解決である。

また、整数の世界においては、「余り」も重要な考え方である。余りの考え方は、時計から時間を読み取るときに使われる。例えば、デジタル時計が 14 時を示している場合、自然と午後 2 時であると判断できる。これは、頭の中で 14 − 12 = 2 という計算をしているからである。



この計算は、12 で割った余りを考えていることにもなる。このように、余りの世界に着目した計算を、**合同式**という。合同式の計算では、「14 と 2 は、12 で割った余りが等しい」という関係を、14 ≡ 2 (mod 12) という形で表す。一見、ただの余りの計算に見えるが、この合同式を使うことで、巨大な数の計算を簡単にしたり、曜日の計算をしたりなど、様々な場面で便利に計算できる。

上で紹介した素数も、合同式も、一見私たちの生活には関係ないように見える。しかし、インターネットを安全に使って通信を行うには、これらの技術は必要不可欠である。私たちがインターネットを介してコミュニケーションをとったり、買い物など金銭のやり取りをしたりする際に、それらの通信は暗号によって守られている。その暗号技術の根幹を支えているのが、**RSA 暗号**であり、これは素因数分解の難しさを利用している。ひと昔は、確かに整数論は役に立たない数学の女王だったかもしれない。情報技術が進化した現代社会においては、整数論は必要不可欠な、真の数学の女王となったのである。