数学は「知性そのものの挑戦」

最先端の研究を背景にした大学の講義を高校生が体験する「明治大学特別授業」が1月31日、福井県立藤島高等学校で開かれた。4月から「研究Ⅱ」の授業でのテーマに数学を選んだ1年生約50人を前に、教壇に立ったのは明治大学総合数理学部の砂田利一教授。「素数と暗号」をテーマに、コンピューターやセキュリティで重要な数学の役割や、古代ギリシャ以来、知性の挑戦として発展してきた数学の歩みを紹介した。

企画制作：福井新聞社 営業局

明治大学特別授業

明治大学×藤島高校

明治大学総合数理学部教授
砂田（すなだ） 利一（としかず）氏
【研究分野】離散幾何解析学と大域解析学
【研究テーマ】さまざまな離散モデルを大域解析学のアイデアを用いて研究。主な研究対象は、結晶中の原子と結合が形作るネットワークや、量子ウォーク、コミュニケーション・ネットワークなど。

実用目的から数の性質の追究へ

数学は、何のために学ぶと思いますか。数学なんて役に立たないという人もいますが、生きていく上で重要な科学技術の背景には、数学がものすごく関係しています。例えばパソコン。分解して集積回路を見ても表面上は分かりませんが、中には数字やグラフ理論、数論など数学が詰まっています。

さて最初は「素数」の話です。数学の歴史は物を数えることから始まり、インドで10進法が発明され、それが2進法などの「b進法」として一般化されました。当初は実用目的だった数学ですが、古代ギリシャでは自然数の性質に興味を示す人たちが現れました。「万物は数である」と言ったピタゴラスは偶数と奇数を区別し、幾何学で知られるユークリッドは、自然数の性質についても記しています。

素数

◉掛け算に関して分解できない数
2、3、5、7、11、13、17、…

◉すべての数は、素数の積として一通りの方法に分解される
（素因数分解定理）
2、3、4＝2×2、5、6＝2×3、7、8＝2×2×2、9＝3×3、10＝2×5、11、12＝2×2×3、13、14＝2×7、15＝3×5、16＝2×2×2×2、17、18＝2×3×3、‥‥

◉**「素数は無限個存在する」（ユークリッド）。**
もし、素数が有限個しかないと仮定して、
それらを $p_1 < p_2 < \cdots < p_n$ とする。
$N = p_1 \cdots p_n + 1$ とおくと、$N > p_n$ であるから N は素数ではない。
したがって、どれかの素数（たとえば p_i）で割り切れるはず
であるが、N を p_i で割ると1余るので、これは**矛盾**。

素数というのは「掛け算に関して分解できない数」つまり、約数が1かそれ自身しかない数です。そして「すべての数は素数の積として一通りの方法に分解される」というのが素因数分解の定理です。ユークリッドは「素数は無限個存在する」ことに気付き、割り算を繰り返して二つの数の最大公約数を短時間で求められる「ユークリッドの互除法」を開発しました。

一方で与えられた自然数が素数かを判定するのは困難です。エラトステネスという人が開発した素数をリストアップする方法は、ものすごい手間がかかります。また自然数の素因数分解を求める計算も長時間を要します。ここは注意しておいてください。

数の理論を発展させた大数学者たち

17世紀にフェルマーという数学者がフランスに登場します。彼は素数をたくさん作りたいと願ってフェルマー数というものを考え、素数の性質についての「フェルマーの小定理」を証明しました。

18世紀に登場した、オイラーというスイス出身の数学者は、フェルマーに影響を受け、素数に関するオイラーの関数や、フェルマーの小定理を一般化する「オイラーの定理」を証明しました。

この後の暗号の話と密接に関係してくるのが、数学史で最も偉大といわれているドイツの数学者、ガウスです。整数論を飛躍的に発展させ、整数の「合同関係」ということを最初に導入し、自然数の性質を分かりやすく説明することができるようになりました。

数学を用いた暗号が社会の安全を守る

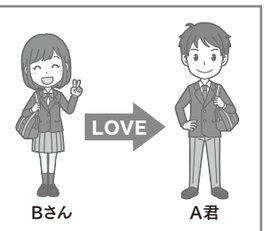
ここからは暗号の話です。暗号とは「第三者に内容が分からないように意志を伝達するため、当事者間で取り決めた符号のこと」で、文字の発明とほとんど同時に発明されました。軍事や外交に用いられ暗いイメージがありましたが、最近は平和な目的でコンピューターやネットワークで広く使われ、社会の安全に重要なものとなっています。

古くから使われてきたのは非公開鍵暗号というもの。暗号を解く鍵を秘密にして、送受信者が共有します。鍵の機密性が重要で、知られると完全に解かれてしまいます。

もう一つ公開鍵暗号という暗号があります。重要な鍵が公開されているにも関わらず、当事者以外の解読が困難な暗号です。最初に考案されたのが、素因数分解の困難さを利用して1977年に発明された「RSA暗号」です。

暗号送付

A君にBさんから秘密の文章を暗号により伝えることを考える。



（1）A君は、2つの大きい素数p,qを選ぶ。
たとえばp＝641,q＝6700417.

（2）A君は、積N＝pqを計算する（N＝4294967297）。
さらに、A君は(p−1)(q−1)＝4288266240と
互いに素であるような、もう一つの数cを選ぶ。
たとえばc＝3.

例として、BさんがA君に「LOVE」というメッセージを暗号で伝える場合。まずA君は二つの大きな素数p、qを選び、その積Nを計算。さらにA君はこのp、qからそれぞれ1を引いた数と互いに素であるもう一つの数cを選びます。A君はp、qを秘密にして、Nとcを誰でもアクセス可能な形にして〝公開された鍵〟とします。

一方でBさんは、A君に知らせたい文章（のアルファベットを）を2進数でコード化し、10進数の自然数Mにします。（逆の変換をすれば）Mから元の文章が分かります。そしてMと、鍵である二つの数を用いて合同関係で計算した数PをA君に知らせます。

A君は公開鍵であるNの素因数を知っているので、ユークリッドの互除法などを用い、短時間でMを求められます。一方他の人は、Nの素因数を知ることは実質的に不可能なため、A君にだけ「LOVE」のメッセージが伝えられます。

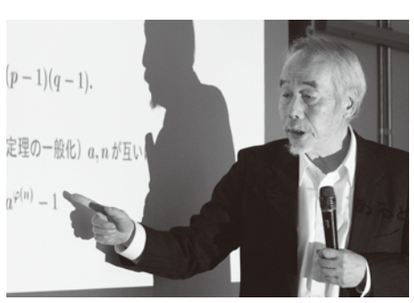
こうした重要な暗号やセキュリティに役立っている自然数の性質は、ユークリッドやオイラー、ガウスらの二千数百年に及ぶ数学の成果です。グーグルの検索も、創始者の1人であるラリー・ペイジ氏が数学理論を用いて適切な結果を表示させる方法を開発しました。ペイジ氏は大金持ちになりましたが、数学者たちはそんなことより、知性そのものの挑戦として素晴らしい数学を作ってきたということを強調したい。皆さんも数学を好きになり、面白い学問だということを理解してください。

明治大学史資料センター所蔵

鯖江市は創立者・矢代操（やしろみさお）の出身地

明治大学は創立者の一人、矢代操の出身地である鯖江市と2011年11月より連携協定を締結し、連携講座や「鯖江ブランド創造プロジェクト」などの取り組みに協力しています。県とも、学生のU・Iターンの促進を目指して就職支援協定を結んでいます。

STUDENT'S VOICES　藤島高校生に聞きました



将来は理学部へ進学し、研究をしていきたい。その上で、研究分野に好奇心を持って課題を自分から見つけていく、意欲や探求心が大切だということに気付くことができた講義だった。（1年男子）

検索エンジンなど便利な技術は、多くの先人の努力と発明があって作られていることを知るとともに、発明や数学の発展が、その先人のチームプレイでなされているのだと気付かされた。（1年女子）

現代の情報通信で、秘密を守るために大きな役割を果たしている暗号にたくさんの数学が詰まっていることを知り、数学が社会に重要な役割を果たしているのだと確かめることができた。（1年男子）

最近、仮想通貨の技術に関する本を読んだこともあり、関心高く聴講できた。数学や科学が、実は身近なところに関係し、用いられているという点が、とても面白く、興味深かった。（1年女子）