私たちの研究室



# 八森祥隆研究室

創域理工学部 数理科学科 准教授
八森（はちもり） 祥隆（よしたか） 先生


八森研のゼミ風景

## 岩澤理論で「もっと大きな数の世界」から楕円曲線を考える

創域理工学部 数理科学科の八森祥隆研究室は、数学の整数論と楕円曲線が研究テーマだ。中でも八森先生の専門は楕円曲線の岩澤理論だ。

楕円曲線は整数論の研究対象の一つで、$Y^2=X^3+AX+B$ という3次方程式で表現され、グラフ化すると平面内の曲線になるものである。

式とグラフを見ると図形の研究にも見えるが、整数論ではA、Bを整数として、この曲線上の座標に「整数点はあるのか？」「有理点、即ち座標が有理数（分数）となる点はどれくらいあるのか？」「素数ごとに見るとどんな性質になるのか？」などの問題を考える。

現代の整数論は整数だけを扱う学問ではなく、整数の性質をより深く知るために、複素数や代数体、群や環などさまざまな数学的概念を道具として使用する。楕円の弧の長さの計算に起源をもつ楕円積分が19世紀に盛んに研究され、その中で楕円積分の被積分関数から定まる複素平面の二重被覆として楕円曲線は現れたが、このような複素関数論的な成果も整数論では利用される。

### 楕円曲線上の有理点

楕円曲線上でX座標とY座標が整数となる整数点は有限個であることが分かっており、$Y^2=X^3-2$ や $Y^2=X^3-X$、$Y^2=X^3+17$ などの具体的な曲線では全ての点を求めることができるが、一般のA、Bに対し整数点を全て求める効果的な方法は知られておらず、その計算はコンピュータでもなかなか困難だ。

一方、有理数の座標を持つ有理点の個数は、有限個の場合も無限個の場合もある。「重要なのは整数ではなく有理数だ」と八森先生は語る。「すでにわかっている1つまたは2つの有理点から、次の操作で新たな有理点を見つけることができる。1つ目はY座標を−Yにすること。2つ目は有理点を通る曲線の接線を引き、曲線と接線のもう一つの交点を求めること。3つ目は、2つの有理点に対し、それらを結ぶ直線を引いて曲線との3つ目の交点を求めること。最初に十分な数の（有限個の）有理点があれば、上記の操作を繰り返すことですべての有理点が発見できる」

しかし、生成元となる有理点を確実に見つけるアルゴリズムは未だに知られていない。また、必要な生成元の個数についても、有名なバーチ・スウィンナートン＝ダイヤー（BSD）予想という、クレイ数学研究所が選定した100万ドルの懸賞がかかる7つの「ミレニアム懸賞問題（Millennium Prize Problems）」の1つがあるが、未解決だ。

このような有理点の理論では、有理点の情報をもち、かつ取り扱いが比較的容易なセルマー群という集合が重要な役割を担う。

### 数の世界を広げる岩澤理論

現在、楕円曲線の研究で有力な方法の一つが岩澤理論だ。整数や有理数は実数や複素数の中にあるが、素数pについてpのn乗が0に収束するp進数体というものにも埋め込まれる。整数論では、このp進数の世界が実数や複素数と同等の重要性を持っている。BSD予想は、楕円曲線に対し定まる「L関数」とよばれる複素関数とセルマー群の間の関係を記述するものだが、そのp進世界での類似が岩澤主予想だ。この類似では、L関数の替わりは「p進L関数」になるのだが、対応するセルマー群の方は、円分的Z_p

拡大という有理数体のｐべき次拡大を積み重ねた無限の塔の上で定まるものを、ガロア群の作用込みで考えたものになる。BSD ではセルマー群をＬ関数のｓ=1 での様子のみで記述する一方、岩澤主予想は代数体が無限の塔の中で拡大していったときのセルマー群の振舞いをｐ進Ｌ関数全体で記述するものとなっており、BSD 予想のｐ進世界における莫大な一般化、精密化であるということができる。

代数体の中で数の性質がどのくらい複雑かを測る指標としてイデアル類群があるが、岩澤理論はもともと、20 世紀半ばに岩澤健吉が発表した、代数体が上へ拡大していったときのイデアル類群の振舞いを調べる理論だ。セルマー群はイデアル類群の類似物と考えることができ、楕円曲線に対しても同様の枠組みで岩澤理論が構築されてきた。

「長々と説明してきたが、私の興味は岩澤主予想というよりは、この無限次拡大体上のセルマー群のガロア群の作用を込めた代数的な構造にある。イデアル類群の構造に関して得られていた既存の結果の類似がセルマー群においても成り立つかや、円分的 Z_p 拡大を他の大きな拡大（非可換拡大など）に変えたときに同様のことが成り立つのか異なる現象が観察できるのか、などについて調べてきた」と八森先生は説明する。

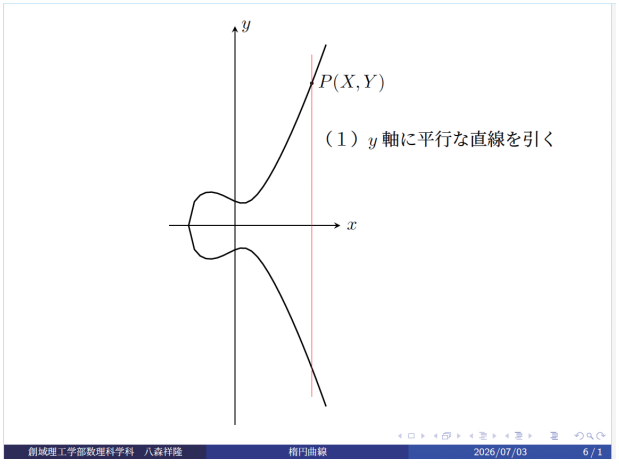
整数論は現在、ラングランズ予想とよばれる巨大な予想を軸に爆発的な進展を遂げている。八森研では、こうした深化拡大を続ける「整数論の世界の片隅で何とか爪痕を残したいとあがいている」のだという。

## 楕円曲線は安全な暗号の作成にも使える

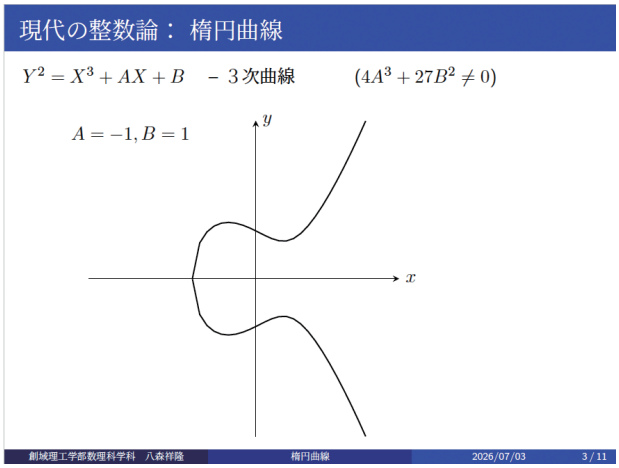
現在八森研は博士課程 1 人、修士 4 人、卒研に取り組む学部生が 9 人という構成だ。同学科では 3〜4 割が大学院に進むが、学部卒での就職先は IT 系や教員などが多い。

博士課程 1 年の岩澤力生さんがこの研究室を選択したきっかけは苗字が岩澤で、同じ名前の岩澤理論の存在を知ったことから興味を抱いた。もともと整数論は好きだったのでイデアル類群の岩澤理論に早くから関心を持ち、現在も研究テーマに選んでいる。「類群の計算はコンピュータを使っても小さい代数体が限界で、下の方で補助的に検証はできるが、上の方の代数体については人間が考えるしかない」（岩澤さん）という。

東京理科大の数学系の学科は理学部と創域理工学部に計 4 つある。数理科学科の独自の特徴として、4 年次に他の学科の研究室の卒業研究に参加し、理工学への応用を学ぶダブルラボというカリキュラムがある。



既知の有理点から新たな有利点を見つけるには 3 つの操作がある



楕円曲線の式とグラフ


岩澤理論は代数体が拡大していったときの数論的対象物の変化を調べる理論だ

修士 2 年の下條孝一さんも、電気電子情報工学科の暗号を専門とする研究室でダブルラボを行った。その経験を経て、現在は楕円曲線の同種写像を利用した暗号を研究テーマに選んでいる。実は楕円曲線暗号は既に広く実用化されており、その発展として同種写像を利用したものが、将来の量子コンピュータによる攻撃にも耐えうる次世代の暗号技術として注目を集め、盛んに研究されているという。

狐塚 淳（インプレスデジタルバリューズ）