教員紹介

今回の「教員紹介」にご登場いただくのは、自然科学系の萩田真理子先生です。萩田先生は理学部数学科に所属され、暗号の開発などにも携わっておられるとか。どうぞインタビューの様子をお楽しみください。

次世代の標準暗号を開発するのが目標です。

Hagita Mariko
萩田　真理子

Q 出身地、ご経歴、ご専門についてお聞かせください

さいたま市出身です。本学の理学部数学科に入学しましたが、実は卒業しておりません。3年生から「飛び級制度」を利用して修士課程に進学しました。修了後、慶應義塾大学大学院理工学研究科博士課程へ進み、学位(博士(理学))を取得しました。その後、慶應義塾大学環境情報学部専任講師、名古屋工業大学工学部講師を経て、本学の情報科学科の助教授に着任し、2012年4月に数学科に異動しました。専門は組合せ論、応用数学です。

Q どんな子ども時代、学生時代を過ごされましたか？ご専門を選択されるようになったきっかけなど含めて教えてください

小さい頃から数えることが大好きでした。数学と物理が好きになって、高校生のときに「数理の翼セミナー」に参加しました。これはフィールズ賞受賞者の広中平祐先生により創始されたもので、各都道府県から一人ずつくらいの数学好きの高校生を集めて、有名な研究者の講演を聴かせてくれるセミナーです。そのときに会った方々が魅力的で親切な方ばかりで、私も数学をやろうと思い、数学科に進学しました。

高校で習う組合せや確率が好きでしたので、大学でも組合せ論を勉強したいと思っていました。私が入学した当時、お茶大の数学科は純粋数学の専門家を揃えている正統派の数学科で、応用数学に分類される組合せ論の専門家はいませんでした。そのためお茶大で代数学を学ぶ傍ら、2年生のときに、グラフ理論で有名な慶應義塾大学の榎本彦衛先生のところに、組合せ論のゼミを見学させてくださいと訪ねていきました。

榎本先生のもとではLint, Wilson著の"A Course in Combinatorics"という本を、私も含めた学生三人で輪講を始めたのですが、半年くらいで他の二人はやめてしまい、一人になってしまいました。そこで当時、榎本先生も参加されていた、毎週土曜日に東京理科大学にグラフ理論の専門家が集まるセミナーがあったのですが、そのセミナーの前に続きを読むことになりました。当時はまだ新しい本でしたが、今では高く評価されている大当たりのテキストだったこともあり、グラフ理論セミナーに集まる方のうち、複数の先生方がセミナー前の時間に行う私の発表を聴きに来てコメントしてくださるなど、大変贅沢なゼミでした。この本を最後まで読み切るのに3年ほどかかり、終わる頃には私は学部を中退して修士課程の院生になっていました。

博士課程は慶應の榎本先生の研究室に進学しました。関連する分野の教員と、博士課程の大学院生も多く集まっている、大変恵まれた環境で勉強することができました。その頃に一緒に勉強した人たちは今も大切な研究仲間になっています。

Q 研究生活で印象深い出来事について教えてください

擬似乱数メルセンヌツイスタ(MT)の提案者の松本眞先生他と共同で、MTを暗号用に変換してCryptMTとFUBUKIという2種類の暗号を作り、ヨーロッパの暗号学会Eurocryptでストリーム暗号の標準を決めるeSTREAMというプロジェクトに応募しました。FUBUKIは選考の前半で候補から外れてしまいましたが、CryptMTは最終選考である第3段階まで残りました。最終的には残念ながら採用されませんでしたが、そういう大規模なプロジェクトに応募して、自分達の開発した暗号がどのように比較、選考されるかというのを見られたのは貴重な経験でした。FUBUKIはストリーム暗号ではなくブロック暗号という別のタイプの暗号に適したアイデアで作った暗号なので、いつかブロック暗号版のFUBUKIを、現在の標準暗号AESに代わる次世代の標準暗号にすることを目標に現在も研究を続けています。

Q ご専門以外のご活動、特に学外でのご活動について教えていただけますか？

お茶大ピアノ班のOG会の演奏会で毎年演奏しています。理学部の教員や研究室の学生にも趣味で楽器を演奏される方が多く、最近は一緒に参加してくださっています。次回は他の教員の方々とご一緒に、ドヴォルザークのピアノ五重奏を演奏する予定です。

最近、物理的な音についても趣味で研究を始めました。今はピアノで和音を弾く時に打鍵する順番によって和音に含まれる倍音の音程が違う理由を、音を聴き比べたり強制振動の式を眺めたりしながら考えています。たとえば、ピアノでファ、ラの♭、ドの和音を弾くときに、響きの中に含まれているファの6倍音、ラの♭の5倍音、ドの4倍音は同じ2オクターブ上のドの音ですが、少しだけ高さが違います。平均律での振動数は、それぞれ、

174.614 × 6 = 1047.68 Hz
207.652 × 5 = 1038.26 Hz
261.626 × 4 = 1046.50 Hz

くらいです。この3つの音を和音で弾くと、最初に弾いた弦の方が後から弾いた弦の音に共鳴してさらに振動するので、倍音のドの音は、先に弾いた弦の出す音の方が大きくなると予想しています。正しければ、どれを先に弾くかで音程が少し変わることになり、ドの4倍音を低めにとりたければラの♭を一瞬早く弾き、高めの方が良ければ一瞬遅れて弾くと良いと考えられます。

Q 最後に、お茶大生に向けてメッセージをお願いします

お茶大生は社交性、協調性に優れた真面目な努力家が多く、大変優秀だと思います。学生の間は、失敗しても成果が上がらなくても良いのですから、もっと自由に何でも興味を持ったことに思い切り取り組んでみて欲しいと思います。卒業後は、どこに行っても好かれるでしょうし高く評価されるでしょうから、自信を持って活躍していってください。

文責：基幹研究院自然科学系　教授
曹　基哲