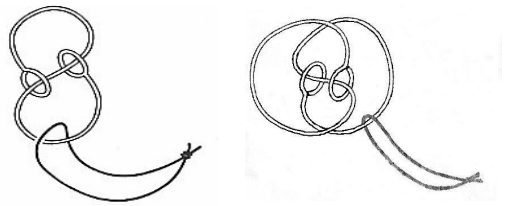
公開講座「情報と数理の世界」

講座内容の紹介

11 月 1 日（金） 解けない知恵の輪　東川和夫 理学部・教授 関数論

知恵の輪とは、その名が示すとおり、なかなか解けないものである。この場合、論理的には、誰がどうやっても、またどれだけ時間をかけても解けない場合と、誰かがうまくやったら解ける場合に分けられる。

では、下の二つは、どれが解けてどれが解けないものでしょうか？



（芦ヶ原伸之の究極のパズル、講談社、1988、p.28）

11 月 8 日（金） 点列の振舞い (決定的とでたらめ的)　小林久壽雄 理学部・教授 確率論

様々な点列$\{a_1,a_2,\ldots\}$が存在する。等差数列、等比数列または漸化式で決まる数列など決定的な数列もあれば、どんな数が現れるか予測できない乱数列、確率的性質は決まっているが、予測困難な確率モデル（ランダムウォーク等の確率過程）もある。一方、点列の点は直線上の点（数）のこともあるし、２次元平面、３次元空間上の点（ベクトル）さらには表とかグラフあるいは絵（関数）を表すこともある。このような点列の振る舞いを PC を通して観察する。数式処理ソフト「Mathematica」と一般的な表計算ソフト「Excel」を使用する。

11 月 15 日（金） 加減乗除から現代暗号まで　木村　巌 理学部・助手

数論本講の前半では、整数の基本的な性質を、厳密な議論によって導く．商と余り、最大公約数、最小公倍数、ユークリッドの互除法、素因数分解の一意性が主題である．また、数を法とする演算を導入する．これらはユークリッドの頃から知られている、普遍的な真理である．20 世紀後半になって、これら基本的な性質に基づいた「暗号」が開発された．数を法とする演算の性質を縦横に使う、ElGaml 暗号、RSA 暗号などを紹介する．これらは、インターネットでの商取引など、ごく日常的に使われている．

11 月 22 日（金） 誤り訂正符号入門　菅谷　孝 理学部・教授 可換環論

符号理論は代数学の基本的な事項，群，環，体についての知識の具体的な応用として格好の素材である．代数学は非常に抽象的な学問であるが，符号理論において実用を見いだす．符号とは，一言でいって，有限体上の有限次元のベクトル空間の部分集合であり，もっとも重要な符号である線型符号は，有限体上の有限次元のベクトル空間である．したがって，有限体という，実数体や複素数体と比較してかなり人工的にみえる体が，実は非常に有用で，実際の通信において本質的な役割を担っている．符号理論，とくにその誤り訂正符号を 2 元体に焦点を絞って講義する．

11 月 29 日（金） 体験　公開鍵暗号 幸山直人 理学部・助手 離散数理

情報化社会と呼ばれる今日、インターネットを通して様々な情報がやり取りされています。しかしながら、その中には個人情報など他人に知られては困る情報もあるため、インターネット上で安全に情報をやり取りする仕組(暗号化)が必要となってきます。現在では、1977 年に MIT の Ron Rivest, Adi Shamir, Len Adleman によって開発された RSA 方式による公開鍵暗号が最も普及しています。この講座では、公開鍵暗号の仕組みを学び、実際に公開鍵暗号を使って安全な電子メールのやり取りを体験していただきます。