数学と工学の意見が食い違う場面は、実に多いのです。水と油とは、まさにこのことでしょう。

直接、言わないまでも、数学の人々は、工学の数学的水準がいかに低いかをあげつらって酒のさかなにしているし、工学の人たちは、数学なんてなんの役にも立たない遊びだと言ってよろこんでいたりします。お互いさまなのです。

数学が思うように役に立たない悔しさ。実務で、思うぞんぶん数学を使ってみたい！
わたしは、すきあらば数学を役立てようと、目を光らせていました。

・・・

しかし、わたしは、仕事上はエンジニアでしたが、中身はエンジニアではありませんでした。効率がアップしたとかダウンしたとかいう話には、ついていけなかったのです。

通勤電車のなかで、ほとんど現実逃避に近い勉強をしながら、わたしはぼんやりと考えていました。数学は、なぜこんなに役に立たないのだろうかと。

コンピュータを利用すれば、19673 くらい一瞬で因数分解できますが、これがもっともっと大きな数になると、話はべつです。

N = 3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

これはどうでしょうか。

答は、

p × q =

1634733645809253848443133883865090859841783670033092312181110852389331001045081512121181675115791900871281664822113126851573935413975471896789968515493666385390880271038021044989571912614655 71

です。コンピュータを利用しても、計算は容易ではありません。

実はこれは、「RSA640」とよばれる、懸賞金付きのチャレンジナンバーです。すでに因数分解されていますから、今からチャレンジしても賞金はもらえませんけれど。

このチャレンジナンバーを因数分解するのに、**2・2GH2 の Opteron プロセッサを 80 台使って、5 カ月近くもかかった**そうです。

これをさらに大きい数にすると、あまりにも時間がかかりすぎるので、「実質的に因数分解できないのと同じ」ということになるのです。

RSA 暗号

というわけで、N を公開してもその因数分解 p×q がはかの人には解けないのですから、p、q を秘密のカギとして利用することができます。この性質を応用したのが、RSA 暗号です。

RSA 暗号の安全性の基礎は、

「掛け算はやさしいけれど、因数分解は難しい」

ということにあります。これだけです。

RSA 暗号を利用すると、閉めるカギと開けるカギを別々のものにすることができます。**閉めるカギを「公開鍵」(N)、開けるカギを「秘密鍵」(p、q)**といいます。大切なことは、このふたつがペアだということです。

名前のとおり、公開鍵は、公開してしまって OK です。誰かに見られてもちっとも困らないカギ、それが公開鍵。

実は、**公開鍵から秘密鍵をつくることはできるけれど、そのためには、公開鍵 N の因数分解（N＝p×q）を解かなければならない**、というところがポイントです。

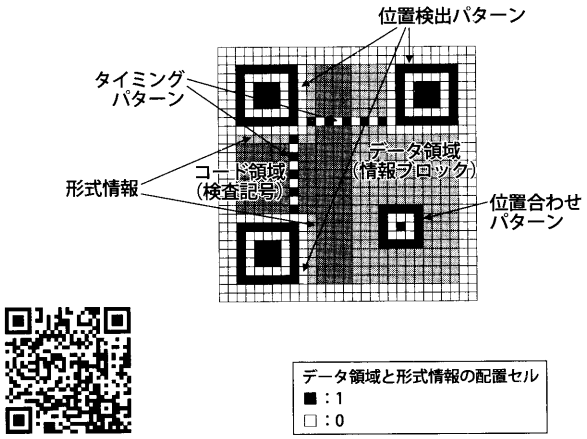

図5　QRコード（型番2、訂正能力M）

QR コードのすごいところは、表面に少々汚れがあっても、正確に読み取ることができる点です。

・・・

実際の QR コードには、**リード・ソロモン符号という優れた誤り訂正符号**が使われています。リード・ソロモン符号は、有限体とよばれる代数学のアイディアを使って構成されています。詳しくは［今井 1990］などの教科書をご参照ください。

まず、津波のスピード。これは、**水深のルートに比例する**ことが知られています。

大陸棚の斜面から外洋に出ると、水深は約 4000 メートルはどになります。そこから津波のスピードを計算してみると、なんと**時速 720 キロメートル**にも達します。

これは音速の約 56%に相当し、はとんど航空機の速度です。このスピードで水の壁が押し寄せてくるのですから、とてつもない現象です。

津波のような波ほ、数学、物理学などの専門用語でほ、**ソリトン**とよばれています。

英語では、soliton と書きます。ソリトンをあえて日本語に訳せば「粒子的振る舞いをする孤立波」　ということになるでしょうか。

ふつう、わたしたちが学校で習う波では、重ね合わせの原理が成り立ちます。重ね合わせの原理とは、つまり、「同じ高さのふたつの波がぴったり重なると、その高さは 2 倍になる」ということです。

いっぽう、重ね合わせの原理が成り立たない世界（1＋1＝2 ではない世界）では、話がまったく違ってしまいます。ソリトンは、重ね合わせの原理が成り立たない世界、つまり、水の波が 1＋1＝2 にならない性質をもっているのです。

フーリエ解析では、音を、基本的な周波数をもった波に分解します。基本的な波というのは、三角関数のことです。

ウェーブレット変換は、ガボール変換のように周波数の分析能力はあまり高くないのですが、そのかわりに変化を見逃しません。ですから、複稚に入り組んだ地層（＝急激な変化）を反映しなければならない地震波の解析にぴったりなのです。宝さがしでは、オートフォーカスの勝ちのようですね。

その後も、ウェーブレット変換の理論は劇的に進歩しました。

石油採掘のはか、画像圧縮、電子透かし（デジタルデータに、著作権データを見えないように組みこむ技術）など、さまざまな分野で応用されています。

確率論と統計学は、わくわくするような具体的な絵が描きにくい分野です（次ページの絵をご覧ください)。

しかし、数学のなかでは人文社会系の分野とのつながりがもっとも深く、応用という観点でみると、**これからますますおもしろくなると予想される分**野でもあります。

アクチュアリーとして活躍するだけであれば、実務能力さえあれば、特別な資格は不要ですが、保険会社の保険計理人になるためには、原則として、日本アクチュアリー会の入会試験を突破して正会員になる必要があります。そのためには、必ずしも数学科を出ている必要はありませんが、数学に加えて、アクチュアリー向けの専門的な勉強（年金、保険など）が必要です。

具体的には、一次試験の「数学」、「生保数理」、「損保数理」、「年金数理」、「会計・経済・投資理論」すべてに合格したうえで、年金、保険それぞれのコースの専門試験を突破しなければなりません。

これは容易ではなく、全科目に合格するのに、**通常は８年から９年を要します**。

数学科数学のキモとは、次のふたつです。

（1）**厳密性**

（2）**一般性**

イプシロン・デルタ論法は、大学数学におけるもっとも巨大なつまずきの石で、多くの学生がここで挫折します。

わたしが大学１年生のころ、数学科の友人たちの多くは、「もう、『てにをは』しか意味がわからん」、「あれが数学なの？」といった反応で、その年の年賀状には「がんばって２年生になりたい……」といった悲鳴が並んでいました。

彼らも、高校までの数学は得意だったはずなのに。わかりにくいという評判は、伊達ではないのです。

しかし、現在では、**複素数なしに振動や波動を扱う工学的問題はうまく解けない**、ということがわかっています。電気回粒の世界でも、「インピーダンス（impedance)」という概念が日常的に利用されていますが、これは、複素数を使って抵抗の概念を一般化したものです。

数学のよくできる学生であっても、プログラミングはぜんぜんできない場合が圧倒的に多く、逆に数学が要り得意でない学生でも、プログラムはかなりよくできる、といった例があるのです。もちろん両方できる学生も、両方ダメな学生もいます。

数学のよくできる学生は、数値計算のアルゴリズムや数式の変形は、十分理解しています。しかし、そのうちのかなりの学生が、それをプログラムできません。

逆に、数学が苦手だけれどプログラムの得意な学生は、式変形もわからないし、アルゴリズムの理解も怪しいのですが、「ようするに、ああやってこうすればいいのか」という部分だけ理解して、さっさとプログラムを組んでしまいます。

情報系の学科を卒業した人、さらに大学院にまで進学した人で、プログラマを志望している人でさえ、プログラミングができないという事実。つまり、少なくとも現時点では、情報系の学科に進学しても、それでプログラミングができるようになる確率はとても低いということです。

結局のところ、プログラミングができるようになるためには、プログラミングの訓練を重ねるほかはありません。これは数学科数学をいくら極めても、現実への応用に結びつかない、という数学の事情とよく似ています

エルデシュ数と同様に、友だちの友だち……というようにしてその分布を調べたら、どうなっているでしょうか。
・・・
mixi でも、隔たりが 5 のところに集中しています。数学者と似て、「世界はせまい」というのは、どうやら本当のようですね。これを、**スモールワールド性**といいます。

現実のネットワークを詳しく解析すると、スモールワールド性だけでなく、クラスタ性という性質があることもわかります。
クラスタ性とは、友人関係でいえば、各人の友達どうしがまた友達どうしである度合いのことです。

社会科学には、現象の核心を突くモデルを提示できる余地がまだたくさん残されており、多くの理工系研究者が魅力を感じていると思われます。

たとえば、工学者のあいだには、
「微分方程式の解法を教える必要はない。なぜなら、マセマティカにかければ答が出てくるからだ。これからはマセマティカだ」という意見があります。
マセマティカというのは、数式を処理したり、数値計算をしてくれるソフトウェアです。
たとえば、解ける微分方程式であれば、ちゃんと答が数式で（！）返ってきますし、そうでない場合でも、近似値で答を求めることができます。実用上はほとんど十分といっていい、たいへん優秀なソフトウェアです。
これは、「算数の計算ができなくても、電卓があるのだから電卓の使い方だけを教えればよい」という主張に近いものがあり、数学者で同意する人はほとんどいないと思います。

たとえば、周波数の解析や画像処理などで多用される**フーリエ解析**。これほ、三角関数がらみの積分計算がたくさん出てきますけれど、**そのほとんどが、高校で習う積分**です。

エンジニアと話をすると、「工学に使えそうな話があっても、数学の専門書を読むと証明のオンパレードで、まったく読めない。なんとかならないものか」という話を聞くことがあります。

そんな話のとき例にあがっていたのは、ウェーブレットですぐれた仕事をした数学者、イングリッド・ドブシーの『Ten Lectures on Wavelety』でした。この本はアメリカ数学会スティール賞の受賞作で、動機づけなどにもページが割かれていますし、たいへん明快な一冊です。

しかし、数学の作法にのっとり、定義、定理、証明のオンパレードになっています。この本を工学者がいきなり読むのは骨が折れる、ということなのです。

数学者からみると非常に素晴らしい本でも、応用する側からみれば、数学的な記号と証明の壁にはばまれて、読みづらい本ということになってしまいます。

こういうとき、エンジニア向けの数学Ⅳの本が必要だな、と思います。この手の本は、数学者が書くと、普遍性は高いものになりますが数学科数学の本になってしまい、エソジニアが書くと、個別の事例の話になってしまって普遍性が損なわれがちです。**数学Ⅳの書き手はなかなかいない**、という気がします。

大数（たいすう）の法則

彼は、大学生のお兄さんが使っている教科書を持ってきて、「これがわかればブラックホールがわかる」と言いました。これは、三平方の定理の一般化なのだと。
テンソルが入り乱れたその公式を眺めながら、**これを理解したいと心の底から思いました。数学を勉強すれば、これがわかるのか。やりたい。理解してみたい！**
なんとかそれを理解したいと思って、それまで行く気のなかった高校への進学を決めたのです。

テンソルとは、ベクトルや行列を一般化したものです。