「虹の数学」を高校・大学で講義して

2021年3月27日（土）15:00-17:00
於数学月間の会ZOOM講演会

真島　秀行
（お茶の水女子大学名誉教授）

1

1

「虹の数学」の切っ掛け・素材

- 専門が複素領域の微分方程式論、不確定特異点を持つ微分方程式の典型例がAiry方程式、George Gabriel Stokesの解析
- 「漸近展開」（大久保健二郎・河野實彦共著、教育出版、1976年2月刊）のまえがきの冒頭に違和感
- お茶の水女子大学理学部数学科同窓会主催講演会（1992年）のネタ
- 科学技術館「科学の祭典」で虹ビーズ、虹シートに出会い、公開講座や学校教材へ

2

2

「漸近展開」のまえがきの冒頭

「東海道新幹線の関ヶ原付近は天候の変化が激しく、虹がよく見られる。学会やシンポジウムの途中に何となく眺めていたが、Stokes現象の古い文献を調べているうちに虹は一本でなく、色の順序が逆である副虹があり、それがこの種の研究の始まりにあたるAiry積分につながることを知った。・・・」

3

3

「虹の数学」の講演・講義

- 大学公開の講演「虹にまつわる数学」（数学セミナー、39(5), 64-68, 2000-05に掲載）
- 日本数学会が関わる「湘南現代数学入門市民講演会」（2001年12月24日14－16、「虹に見える漸近解析」（数学通信7－2、2002）
- 附属高等学校と大学との高大連携プロジェクト（2002～）「教養基礎（数学）」（虹の数学）
- 大学での講義「数理のことば」（15回講義）中の1～2回分など

4

4

虹は文系的にも十分興味深い

- 「虹にまつわる数学」（数学セミナー、39(5), 64-68, 2000-05）冒頭に民俗学的な話題もあり文系的にも十分興味の対象だが、ここでは理系的な興味で説明したい、と書いた。
- 虹の色がいくつかなど民族によって違うこと（例えば、鈴木孝夫（2021年2月10日死去）氏の「ことばと文化」（岩波新書、1973年5月刊）や虹に対して抱く印象、感情、迷信など（例えば、「銀河の道　虹の架け橋」（大林太良著、小学館、1999））

5

5

「虹の数学」の高校の講義

- 附属高等学校の「教養基礎（数学）」（虹の数学）は2002年試行から始めた。附属高等学校の教諭の方たちと第1学年と第2学年にまたがる“科目”として、数学Ⅰの三角比、数学Ⅱの三角関数等にうまく繋げ、光路の作図（コンパスと物差し、数式処理ソフト）の高等学校教諭の指導を加えて組み高等学校の数学の教育課程を大幅に変えることは意図せず、初期には俯瞰講義と“虹シート”の作成、観察の演習と2回分、後に最初と最後の2回分を担当

6

6

「虹の数学」の高校の授業

- 「教養基礎（数学）」（虹の数学）の第1学年の第1回「虹の数学」と第2学年の最終回「虹の彼方に何があるか」と題して講義を担当
- その間に数学Ⅰの三角比、数学Ⅱの三角関数、その他に、二次曲線、円周角の定理の逆、三角関数の微分、統計の相間係数とベクトルの内積の関係等、光路の作図（コンパスと物差しで第1学年で、数式処理ソフトで第2学年で高等学校教諭の指導を併せて構成

7

7

「虹の数学」の評価

- 「教養基礎（数学）」（虹の数学）の第1学年、第2学年の授業評価は毎年生徒アンケートを集計、分析
- 個々の事実より重視したのは次のこと:

「虹の数学」の学習を通して、虹という現象を知るために、数学が役に立つということが実感できた。
「虹の数学」の学習を通して、虹という現象を知るために、数学だけでなく物理、化学、生物など色々な科学の知識が必要であると実感できた。
「虹の数学」の学習を通して、数学、物理、化学、生物は、他の現象を理解する為にも役立つことが実感できた。

8

8

教養基礎教育（数学）
虹の数学

- 講演会では別のpptにより行なった。
- 真島秀行、「虹にまつわる数学」、数学セミナー、39(5), 64-68, 2000年5月、参照のこと

9

9

教養基礎科目（数学）
虹の彼方に何があるか

（新型コロナウイルス感染防止措置により
講演中止による特別配付用）

真島　秀行
（お茶の水女子大学名誉教授
元大学理学部数学科教授
元副学長、元附属中学校長）
2020年2月27日（木）11：42-12：27

10

10

2018年入学式の校長祝辞

「皆さんはIPS細胞のように見える。何にでも成れる無限の可能性を秘めている。」

- 私も前の附属学校担当副学長、前の附属中学校長として入学式に参列し皆さんの入学を祝福しました。さらに数学の見方・考え方、数学的な問題解決力、統計的な問題解決力が付くとさらに可能性が高まると私は考えています。

11

教養基礎数学「虹の数学」も皆さんと同じ“2002年”生まれ

- 皆さんは、2002年4月2日から2003年4月1日生まれだと思います。
- 教養基礎数学「虹の数学」もその頃に検討が始められ2004年から授業が始まりました。
- 今の形態の教養基礎は2019年度入学生までで2020年度入学生からは違う形態にすることを検討しSSH校にも指定され変更しました。
- 皆さんとは2年生の終わり頃、2020年の2月頃に「虹の数学のまとめ」の授業をしにまた来ます、と昨年5月7日の初授業で予告しました。

12

社会の変化

- 2019年4月30日で平成の時代は終わり、2019年5月1日から令和の時代になり、天皇即位関連行事が挙行され、天皇誕生日の祝日も12月から2月に移動しました。新しい元号の時代になり、社会は狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く、**サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会**（Society5.0）へ向かっています。 ~13

13

桜はなぜ「〇割咲き」でなく、「〇分咲き」なのか

- 2017年の桜の開花は暖冬でやや遅めの3月下旬らしいです。ところで、昨年2016年2~3月に皆さんの先輩に「割・分」という用語について質問を受け、最終的には、“桜はなぜ「〇割咲き」でなく、「〇分咲き」なのか”という日経新聞電子版20160323記事になっています。
- 2007年附属中学校、2010年に附属高等学校卒業の方で、附属高校時代に“虹の数学”を勉強し、三角関数は苦手だったが、光路を描いたりして楽しかった、と言ってくれました。 14

14

「虹の数学」で何をしてきたか0

0．虹という自然現象の発生原理に潜む数理を解説し、高校数学をほとんど使うことからそれを学ぶ動機となることを話した。例えば、

〇（正弦関数で表される）スネルの法則

〇太陽光による虹の曲線は（平行線の錯角が等しいことなどを使うと円錐の断面）二次曲線

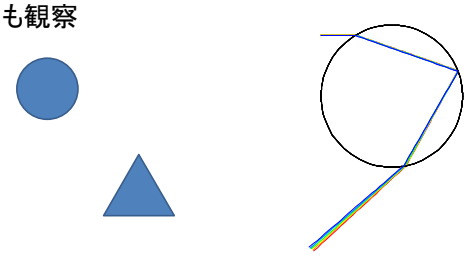
〇点光源による虹の曲線は円周角の定理（の逆）などを使うとできそこないトーラスの切断線（四次曲線）

●また虹の解明には理学が総動員されることも

15

「虹の数学」で何をしてきたか1

1．虹シートを作成し、人工虹を観察、球形レンズやプリズムなどで光がどんな風に見えるかも観察



16

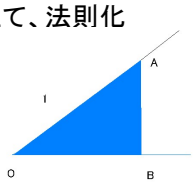
16

「虹の数学」で何をしてきたか2

2．光の屈折の原理（スネルの法則）の学習

2．1　物理的に実験し、仮説を立て、法則化

2．2　三角比、三角関数の学習

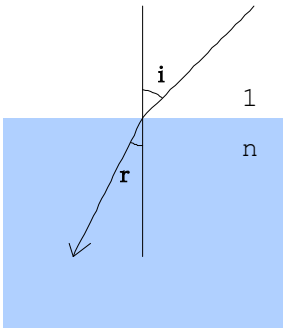


$$\cos\theta=\frac{\mathrm{BO}}{\mathrm{AO}},\sin\theta=\frac{\mathrm{AB}}{\mathrm{AO}},\tan\theta=\frac{\mathrm{AB}}{\mathrm{BO}}$$

17

17

スネルの法則　sin i　= n sin r



18

18

「虹の数学」で何をしてきたか3

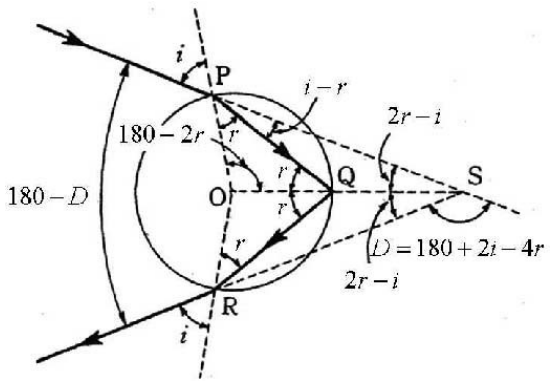
3．水と空気の間の屈折率が4/3であるとして、理想的に水滴が球だとモデル化して光がどのように通過するか、光路を描く

3．1　1年生では、コンパスと定規で作図

3．2．2年生でコンピュータで数式処理ソフト（Mathematica）を使って描く

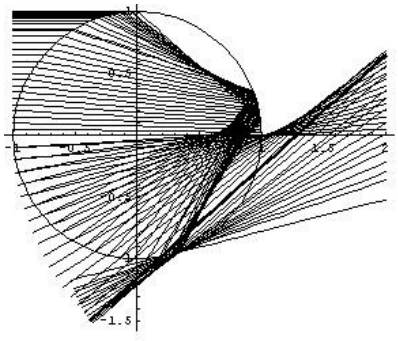
19

19



20

焦線



21

21

「虹の数学」の先にあるもの

○過剰虹の発生原理
— エアリー関数の挙動
○多次元虹
— カタストロフ

○光（電磁波）の科学（物理学、化学、生物学、医学、工学・・・）

22

22

過剰虹とエアリー関数

この虹の写真を見ると紫色の帯が2～3度繰り返しているのがわかる。
これを過剰虹という。この現象を屈折、反射等の幾何光学では説明できない。
回折を考慮して太陽光が滴を通過したあとの上空近くの光になるかを
明らかにしなければならなかった。Airyは、積分で定義された関数を導入し、
その原点付近の挙動を調べ、Stokesがその関数の満たす微分方程式を複素平面上で考察することにより、
正の無限大の向きには0に漸近し、負の無限大の向きには正弦関数のような挙動を示すことに成功した。

$$\int_0^\infty \cos\frac{\pi}{2}(t^3 - xt)dt$$

$$\frac{d^2}{dz^2}u - zu = 0,$$

$$Ai(x) = \frac{1}{3^{2/3}\Gamma(\frac{2}{3})}[1 + \frac{x^3}{2\cdot 3} + \frac{x^6}{2\cdot 3\cdot 5\cdot 6} + \frac{x^9}{2\cdot 3\cdots 5\cdot 6\cdot 8\cdot 9} + \cdots]$$
$$-\frac{1}{3^{1/3}\Gamma(\frac{1}{3})}[1 + \frac{x^4}{3\cdot 4} + \frac{x^7}{3\cdot 4\cdot 6\cdot 7} + \frac{x^{10}}{3\cdot 4\cdot 6\cdot 7\cdot 9\cdot 10} + \cdots],$$

23

23

$$z^{-\frac{1}{4}}\exp\left(-\frac{2}{3}z^{\frac{3}{2}}\right)\sum_{n=0}^{\infty}\frac{\Gamma\left(3n+\frac{1}{2}\right)}{(2n)!}\left(\frac{i}{3z^{\frac{3}{4}}}\right)^{2n}$$

$$z^{-\frac{1}{4}}\exp\left(\frac{2}{3}z^{\frac{3}{2}}\right)\sum_{n=0}^{\infty}\frac{\Gamma\left(3n+\frac{1}{2}\right)}{(2n)!}\left(\frac{1}{3z^{\frac{3}{4}}}\right)^{2n}$$

24

漸近挙動

- , **$x>0$ で指数関数的に減少し，$x<0$ では，正弦関数のように振動する**関数であることを示し，**アレクサンダー暗帯の存在と過剰虹の発生**とを説明した．それは同時に，今日**ストークス現象**といわれることの発見でもあった．

25

$$Ai(z) \approx \frac{1}{2\pi} z^{-\frac{1}{4}} \exp\left(-\frac{2}{3} z^{\frac{3}{2}}\right) \sum_{n=0}^{\infty} \frac{\Gamma\left(3n+\frac{1}{2}\right)}{(2n)!} \left(\frac{i}{3z^{\frac{3}{4}}}\right)^{2n}$$

$$Ai(z) \approx \frac{1}{2\pi} z^{-\frac{1}{4}} \exp\left(-\frac{2}{3} z^{\frac{3}{2}}\right) \sum_{n=0}^{\infty} \frac{\Gamma\left(3n+\frac{1}{2}\right)}{(2n)!} \left(\frac{i}{3z^{\frac{3}{4}}}\right)^{2n}$$

$$+ \frac{i}{2\pi} z^{-\frac{1}{4}} \exp\left(\frac{2}{3} z^{\frac{3}{2}}\right) \sum_{n=0}^{\infty} \frac{\Gamma\left(3n+\frac{1}{2}\right)}{(2n)!} \left(\frac{1}{3z^{\frac{3}{4}}}\right)^{2n}$$

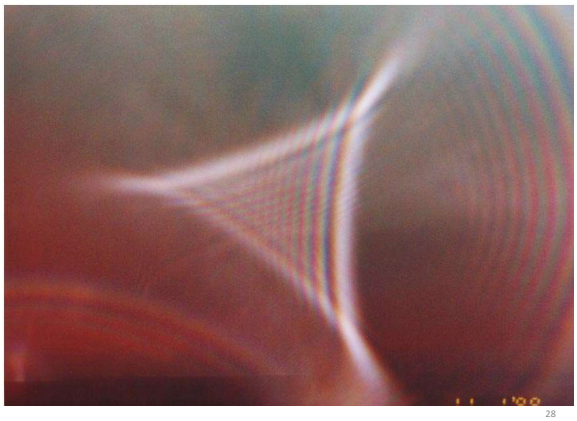
$$Ai(-x) \approx \frac{1}{\pi} x^{-\frac{1}{4}} \sum_{n=0}^{\infty} \frac{\Gamma\left(3n+\frac{1}{2}\right) \sin\left(\frac{2}{3}x^{\frac{3}{2}} + \frac{\pi}{4} - \frac{n\pi}{2}\right)}{(2n)!} \left(\frac{i}{3x^{\frac{3}{4}}}\right)^{2n}$$

26

カスプ虹など

- 前にカップにできる焦線の図を見たが，実はこのような形の‘虹’もとらえらることができる．**カスプ虹**とよばれるもので，滑らかな凹凸のあるガラスに懐中電灯の光を絞って当て，シャッターを開いたままで撮影すればよい．技術を習得するのに多少苦労するが面白い体験ができる，と思う．

27



28

28

$$V = \frac{x^3}{3} + vx$$
(fold singularity)

$$V = \frac{x^4}{4} + \frac{u}{2}x^2 + vx$$
(cusp)

$$V = \frac{x^5}{5} + \frac{u}{3}x^3 + \frac{v}{2}x^2 + wx$$
(swallow tail)

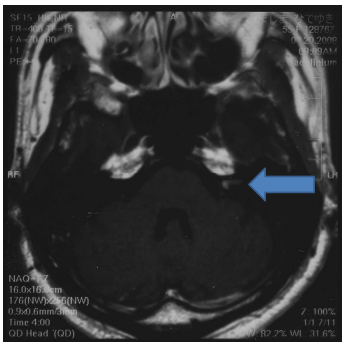
$$V = \frac{y^6}{6} + \frac{t}{4}y^4 + \frac{u}{3}y^3 + \frac{v}{2}y^2 + wy$$
(baterfly)

$$V = x^3 + y^3 + wxy - ux - vy$$
(hyperbolic umbilic)

$$V = x^3 - 3xy^2 + w(x^2 + y^2) - ux - vy$$
(elliptic umbilic)

29

MRIによる頭の断面図（聴神経腫瘍）



30

学習指導要領との関わり

- 高校のほとんどの単元と関わりがある。
- 確率、統計についても、虹の発生頻度、見られる確率を考えるなど、関連を考えられ、実際、2015年から虹予報なるものが滋賀県で出されるようになった。
- 外部講師による統計の応用に関する講演会も実施してきました。
- 大学入試センター試験の数学Ⅰ・数学Aの必答問題に統計の出題があります。

31

31

滋賀県虹予報（2015年10月9日）

32

虹予報1

- 虹が出やすいとされるびわ湖に多くの観光客を呼び込もうと、滋賀県は2015年10月9日から全国で初めてとなる「虹予報」を始めました。
- 滋賀県によりますとびわ湖は山に囲まれているためにわか雨が多く、虹が出る環境に恵まれているということです。
- 県などではこの、びわ湖の虹をPRして観光客の誘致につなげようと、民間の気象会社と協力して全国で初めての「虹予報」をインターネットで発表することにしました。

33

33

虹予報2

- 虹予報はびわ湖周辺の7つの地域について、虹が発生する確率を0から7までの8段階で表示します。
  2015年10月9日はJR東京駅のイベントスペースで、三日月知事などが出席して1回目の「虹予報」が発表され、9日と10日は全域で虹が見られる可能性が低い「0」でした。
- 発表を見ていた東京都の女性は「虹が出るとうれしい気持ちになるし元気をもらえると思うので、虹予報でいつ出るか分かると見たくなります」と話していました。

34

34

虹予報3

- 三日月知事は、「美しくて、はかない虹を楽しみながら、びわ湖周辺の旅を心に残して楽しんでもらえるよう、情報をしっかり発信していきたい」と話していました。
- 「虹予報」は、毎朝6時半に発表されます。

（2015年10月09日　20時32分）

- 「虹の数学」のカリキュラムを作る際、前の高校の先生にはULMにいた時（2002年10-2003年1月）、10月は結構何度も虹が見え、統計データを作ろうと思ったことがあり、統計との関わりはこのあたりにあると説明していた。

35

35

滋賀県虹予報（2015年10月9日）

36

身近な対象として考えられるもの

- 自然現象：虹、生物（フィボナッチ数列が現れる、黄金比、対称性、初等カタストロフ、フラクタル）
- 実用人工物と非実用人工物：暦、地図、音階、人工衛星（GPS、ナーナビ、携帯電話のGPS機能も含めて）、計算機、人工知能、ネットワーク、ゲーム・パズル
- 人間社会生活：経済（金利、バーコード、価格設定、商品検査；製造（車、鉄道、半導体、コンピュータ）、金融、保険、製薬、）、政治（選挙、意思決定・ゲームの理論）、医療（検査法、手術法、人工心臓、伝染病）、環境（気候・地球温暖化、人口）

37

ガリレオの「偽金鑑識官」のことば

- 「・・・哲学は、眼のまえにたえず開かれているこの最も巨大な書（すなわち、宇宙）のなかに、書かれているのです。しかし、まずその言語を理解し、そこに書かれている文字を解読することを学ばないかぎり。理解できません。その書は数学の言語で書かれており、その文字は三角形、円その他の幾何学図形であって、これらの手段がなければ、人間の力では、そのことばを理解できないのです。それなしには、暗い迷宮を虚しくさまようだけなのです。」

38

38

ガリレオのことばを端的に言えば

自然は数学ということばで書かれている

39

39

小平邦彦のことば

- **小平邦彦の言葉（『怠け数学者の記』の「数学者の妄想」より）**
- **「数学は森羅万象の根底をなしている。数学は自然科学に実に不思議なほど役に立つ。しかも多くの場合、自然科学の理論に必要な数学はその理論が発見されるはるか以前に予め数学者によって準備されていたのである。――私は物理現象の背後に数学的現象が実在していると思うのである。」**

40

40

小平邦彦のことばを短くいうと

森羅万象の根底に数学は実在する

41

41

数理が隠れている例１　暦

- 暦を作るというためには多くの数理的な考察が必要である。

―1太陽年（太陽が春分点を通過してから再び春分点を通過するまでの時間、365.24219879日）、1朔望月（月の満ち欠けの周期、29.530589日）、１日、１時間、1分、1秒を決めること。

―太陽暦（閏年をどうおくか）

―（旧暦）太陽太陰暦（閏月をどうおくか）

42

42

太陽暦の閏年の置き方

- 日本で今使っているのは太陽暦。
- 太陽暦にも、いくつか種類あって、グレゴリオ暦、すなわち、次のような規則によるもの

―通常、1年を平年365日とする。

―4で割れる4年ごとに閏年をおいて366日とする

―ただし、100で割り切れる場合、その商がさらに4で割り切れない年は平年とする。

- 1700年、1800年、1900年は平年、2000年は閏年。400年間に3回は閏年でなく平年とする

43

太陽太陰暦

- 太陽太陰暦は新月を月の初めとし、さらに季節の変化に順応するように太陽の運行も考えて調節してつくる。
- 月の初めが、ついたち（朔日）、
- 月の終わりが、みそか（三十日、晦日）
- 29日と30日の月を交互に6か月ずつ置き、平均29.5日にした。しかし、それでは1太陽年に１１日くらい違い２～３年に一度閏月を入れた。また、季節示すため、二十四節気を置き目安にした。

44

二十四節気

- 昼夜の長短を基準にした季節区分（各季節の中間点）- 春分・夏至・秋分・冬至
- 昼夜の長短を基準にした季節区分（各季節の始期）- 立春・立夏・立秋・立冬
- 気温 - 小暑・大暑・処暑・小寒・大寒
- 気象 - 雨水・白露・寒露・霜降・小雪・大雪
- 物候 - 啓蟄・清明・小満
- 農事 - 穀雨・芒種

45

暦の曜日

- 月火水木金土日は、日月に火水木金土をあわせて7つにしている。
- 7日ごとにもとにもどるようにしている。
- 曜日パズルを作ろう。例えば

Q.2014年4月1日は火曜日、では、2014年7月1日は何曜日？

Q.9月1日が月曜日なら12月1日は何曜日？

Q.10月24日が金曜日なら12月5日は何曜日

46

1900年代の曜日計算1

- 1900＋X年m月n日の曜日の計算公式は次のよう：m月に対して、キーナンバーm′を次のように定める

m 1 2 3 4 5 6 7 8 9 10 11 12

m′ 0 3 3 6 1 4 6 2 5 0 3 5

- X+[X/4]+m′+n の7で割った余りを x とすると

x	0	1	2	3	4	5	6
曜日	日	月	火	水	木	金	土

47

1900年代の曜日計算2

- ただし、閏年の1月と2月については

x	0	1	2	3	4	5	6
曜日	土	日	月	火	水	木	金

(1900年1月1日は月曜日だった)

- m月に対する、キーナンバーm′は、その年のその月前までの合計日数を7で割った余り

m 1 2 3 4 5 6 7 8 9 10 11 12

m′ 0 3 3 6 1 4 6 2 5 0 3 5

48

数理が隠れている例2　地図

- GPS（全地球測位システム）を利用して、位置情報を獲得できるようになっています。

ー3つの球の交点は2つであること、

ー距離（関数）を近似的に一次関数にして連立方程式の近似解をもとめること（大学レベル）

- カーナビ、携帯電話の位置情報に利用されている。
- 地図を作るための測量にも利用されている。

49

49

数理が隠れている例2　地図

- GPS（全地球測位システム）を利用して、位置情報を獲得できるようになっていま

地震の震源地を見つけるための原理

ー3つの球の交点は2つであること、

ー距離（関数）を近似的に一次関数にして連立方程式の近似解をもとめること（大学レベル）

- カーナビ、携帯電話の位置情報に利用されている。
- 地図を作るための測量にも利用されている。

50

50

数理が隠れている例2　地図

- GPS（全地球測位システム）を利用して、位置情報を獲得できるようになっていま

地震の震源地を見つけるための原理

ー3つの球の交点は2つであること、

ー距離（関数）を近似的に一次関数にして連立方程式の近似解をもとめること（大学レベル）

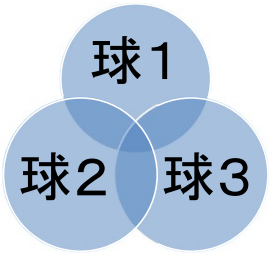
- カーナビ、携帯電話の位置情報に利用されている。自動車の自動運転にも。
- 地図を作るための測量にも利用されている。
- 赤色立体地図で中世の山城発見もあった。

51

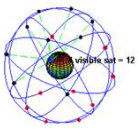
51

GPSの数学的な原理1

3つの球の交点は2つ、誤差評価のため人工衛星4つ使用



地球の半径約　6400kmに対して高度2万kmに人工衛星の静止軌道があるので、赤道上に90度ずつ離して4点と北極と南極にそれぞれ1点、合計6点あれば地球上のどの位置でも交信可能、よって、
4×6=24個を適切に配置する



52

52

GPSの数学的な原理2

- 空間座標を用いて、地球上の不明な1点 (x, y, z) と4つのGPS衛星の位置 $(a_j, b_j, c_j)(j = 1,2,3,4)$ との距離は次で表される。 $\sqrt{(x-a_j)^2+(y-b_j)^2+(z-c_j)^2}$
これを（大学で習う）微分可能な関数のテイラー展開を使って近似的に一次式で置き換え、誤差項も含んだ4元4連立方程式を近似的に求める。（連立方程式は中学校でも習う）

$$
\begin{aligned}
p_1(x-a_1)+q_1(y-b_1)+r_1(z-c_1)+u &= s_1\\
p_2(x-a_2)+q_2(y-b_2)+r_2(z-c_2)+u &= s_2\\
p_3(x-a_3)+q_3(y-b_3)+r_3(z-c_3)+u &= s_3\\
p_4(x-a_4)+q_4(y-b_4)+r_4(z-c_4)+u &= s_4
\end{aligned}
$$

53

数理が隠れている例3　暗号

- インターネット取引などでは、個人情報の安全性を守るために、暗号を使っている。
- たとえば、RSA暗号は、大きな自然数の素因数分解が非常に時間がかかって困難であることを安全性の根拠としている。（56＝7×8, 131337=9×145973, 6860731=47×145973, 段々桁数が大きくなると難しくなる。）
- また、暗号化、復合化は、フェルマーの小定理、（数論における）オイラーの定理などを用いる。

54

54

RSA暗号の由来

- 1977年に発表されたロナルド・リベスト(Ron Rivest)、アディ・シャミア(Adi Shamir)、レオナルド・エーデルマン(Len Adleman) の3名の共著者の頭文字をつなげてこのように呼ばれる。当時、デフィーとヘルマンによって発表されたばかりの公開鍵暗号という新しい概念に対し、秘匿や認証を実現できる具体的なアルゴリズムを与えた。

55

RSA暗号の仕組み

- RSA暗号は次のような方式である：鍵ペア（公開鍵と秘密鍵）を作成して公開鍵を公開する。まず、適当な正整数 e（通常は小さな数。65537 (=2^{16}+1) がよく使われる）を選択する。また、大きな2つの素数{p ,q }を生成し、それらの積 n (=pq) を求めて、{e, n }を平文の暗号化に使用する鍵（公開鍵）とする。2つの素数{p ,q }は、暗号文の復号に使用する鍵（秘密鍵）d ($de \equiv 1 \pmod{(p-1)(q-1)}$)の生成にも使用し、秘密に保管する。

56

RSA暗号の暗号化と復号化

- 暗号化（平文 m から暗号文 c を作成する）:

$$c \equiv m^e \pmod{n}$$

- 復号（暗号文 c から元の平文 m を得る）:

$$m \equiv c^d \pmod{n}$$

- ここで a と b を n で割った余りが等しいことを次のように表した.

$$a \equiv b \pmod{n}$$

57

RSA暗号の例題

- 素数 $p=2$，素数 $q=5$ とし，$n=pq=2\times5=10$ とする．10 以下の自然数で 10 と互いに素な自然数は1，3，7、9で、その個数は4である．4 と互いに素となる自然数を$e=3$ とする$\{e,n\}$＝{3, 10 }を平文の暗号化に使用する鍵（公開鍵）とし,$de\equiv1(\mathrm{mod}.4)$となる$d=3$ を秘密鍵として保管する.
- 平文 $m=2$ から計算して$c=8$を暗号とする.
- 暗号 $c=8$ から と計算して$m=2$ と平文を復号できることがわかる.

58

RSA暗号の安全性

- ここで、暗号化（e 乗）は、{e, n }があれば容易に計算できるのに対して、復号(e 乗根)は、「n の素因数を知らないと難しい（大きい合成数の素因数分解も難しい）」と考えられている。つまり秘密鍵を用いずに暗号文から平文を得ることは難しい、と信じられている。これがRSA暗号の安全性の根拠である。しかし最近、量子コンピュータが実現し計算速度が格段に向上しており、安全なままであるかは分からない。

59

数理が隠れている例4　AI

以下、松原望著「ベイズの誓い」ーベイズ統計学はAIの夢を見る」より）

- ベイズ統計の推定は直観に則しているもですが、数字をもって説明すると説得力が出てきます。これは観測されたデータから、自然の法則を知ろうとする、科学の姿勢そのものでもあります。また、第二次世界大戦中は敵軍の潜水艦の位置を推定するのにも使われました。保険や金融など、経済の世界でもベイズの定理は使われています。

60

60

次期数学A （2）場合の数と確率からベイズの統計を解説した部分

- …なお，この条件付き確率の式（一般的な確率の乗法定理）は，原因となる事象が生じた際に結果が生じる確率を計算する方法として，すべての確率に対して基本的な考え方となる。また，この式は，結果が生じたときに原因が生じている主観確率を計算するベイズの定理を導く基になる考え方でもあり，次のようなベイズ統計の基本的な考え方を知った上で指導に当たることも，生徒の確率の意味の理解を深めるために有用であると考える。

61

61

次期数学A （2）場合の数と確率からベイズの統計を解説した部分（続）

- まず，データを観測する前に関心のある事象に主観確率（事前確率）を与え，関心のある事象が生じた下での観測データが出現する客観的条件付き確率（標本確率）を求めて乗法定理に基づき掛け算をする。それを用いて，関心のある事象のデータ観測という条件付き主観確率（事後確率）を推定する。これがベイズ統計の基になる考え方である。
- **例：3つの袋に赤玉と白玉が入っていて白玉を取り出す確率がどの袋から取り出すと高いか、という問題（例：松原望著「ベイズ統計学」、「ベイズの誓い」参照）。**

62

62

壺と玉の問題（取り出された玉の色【結果】から玉の出所【原因】を推定する例題）

- つぼがA,B,Cの3つあり、その中に赤玉、白玉それぞれ比率3：1，1：1，1：2で入っている。
- ここからランダムに取り出された玉が「赤」だったとしたら、この玉はどこからやってきたであろうか？赤玉がいっぱい入ったAか、いやCの可能性だってきっとある。どの壺から出てきたのか、今はわからない。だから事前確率は一様に等しくAもBもCも3分の1とする。

1/463

63

壺と玉の問題（取り出された玉の色【結果】から玉の出所【原因】を推定する例題）(続)

- 条件付き確率の公式から、3/4×1/3＋1/2×1/3＋1/3×1/3= ¼＋1/6＋1/9 = 19/36
- これからベイズの定理から事後確率はそれぞれ1/4÷19/36=9/19、1/6÷19/36=6/19、1/9÷19/36=4/19
- 従って、Aの壺からの確率が高いと推定される。

1/464

64

壺と玉の問題（取り出された玉の色【結果】から玉の出所【原因】を推定する例題一般化）

- 壺がA,B,Cの3つあり、その中に赤玉、白玉それぞれ比率3：1，1：1，1：2で入っている。
- ここからランダムに取り出された玉が「赤」だったとしたら、どの壺から出てきたのか、事前確率としてA，B，Cの順にa, b, c (a+b+c=1)とする。
- 条件付き確率の公式から、p1=3/4×a＋1/2×b＋1/3×c
- ベイズの定理から事後確率はそれぞれ，3a/4÷p1, b/2÷p1, c/3÷p1，となる.
- これを事前確率として再び事後確率を求めると，条件付き確率の公式から、p2=3/4× 3a/4÷p1 ＋1/2× b/2÷p1 ＋1/3× c/3÷p1=(3/4× 3a/4＋1/2× b/2＋1/3× c/3)÷p1
- ベイズの定理から事後確率はそれぞれ，3/4× 3a/4÷p1 ÷p2, 1/2 × b/2÷p1 ÷p2,, 1/3× c/3÷p1 ÷p2, となる.
- すなわち，3/4× 3a/4÷(3/4× 3a/4＋1/2× b/2＋1/3× c/3), 1/2 × b/2÷(3/4× 3a/4＋1/2× b/2＋1/3× c/3), 1/3× c/3÷(3/4× 3a/4＋1/2× b/2＋1/3× c/3), となる.

1/465

65

壺と玉の問題（取り出された玉の色【結果】から玉の出所【原因】を推定する例題一般化）

- 次々に更新していくとn回目の事後確率は，次のよう：
  $(3/4)^n a \div ((3/4)^n a + (1/2)^n b + (1/3)^n c)$,
  $(1/2)^n b \div ((3/4)^n a + (1/2)^n b + (1/3)^n c)$,
  $(1/3)^n c \div ((3/4)^n a + (1/2)^n b + (1/3)^n c)$,
- 従って更新を続けていくと事後確率の極限は次のようになる：aが0でなければ，1，0，0，a=0で，bが0でなければ，0，1，0，a= b = 0でc=1ならば，0，0，1のままである.
- この例が示唆するのは，事前確率が“適切でない”と更新しても妥当な結果が得られないので，事前確率はやはり適切に与える必要がある，ということであろう．なお、この例ではサンプルサイズが小さいのでこうしたことが起きたが、大きければどんな事前確率から始めても真の値に近づいていくというベイズ統計学におけるサベジの定理もがある.
- （L.J. Savage のPrecise Measurement or Principle of Stable Estimation、サンプルサイズが大きくなれば，任意の事前分布に対して事後分布は真の値の近くに収束するというもので，ベイズ統計の有用性を保証する重要な性質．ただし，事前分布の Support は全母数空間をカバーする必要がある．3つの壺の話は，小標本の場合で，事前分布の設定が結論に影響するのは当然である．）

1/466

66

数学とは（科学技術の智プロジェクトに於けるまとめ）

1．数学の基礎は数と図形である。さらに、変化と関係、データと確からしさも対象とする。

2．数学は抽象化した概念を論理によって体系化する。

3．数学は抽象と論理を重視する記述言語である。

4．数学は普遍的な構造（数理モデル）の学として諸科学に開かれている。

67

67

すなわち、数学は・・・

- 数学はそれ自身、一つの学問分野であり、研究され新しい概念を生み発展している。
- また、数学は諸科学のことばとしても発展し続けている。ガリレオの時代に、自然科学を記述することばとして使われることが認識され始め、現在は経済学などの社会科学、心理学などの人文科学へも応用されている。
- さらに、小学校・中学校・高校で数学の科目として習う“統計”は現状分析、課題発見、課題解決などに役立つ手法を提供してくれる。

68

68