文化としての数学を

LADy SCIENCE BOOKLET

1

文化としての数学を

吉田信也

CORE of STEM 2015

はじめに

本ブックレットは、私が奈良女子大学附属中等教育学校の 5 年生(高校 2 年生)に開講した学校設定科目「コロキウム」の講座「文化としての数学を」用に作成したテキストである。

奈良女子大学附属中等教育学校は、文部科学省より 2005 年度～2009 年度、2010 年度～2014 年度の 2 期に渡りスーパーサイエンスハイスクール(SSH)に指定され、研究を続けてきた。「コロキウム」は、第 2 期 SSH における研究の柱の 1 つとして実践されてきて、2014 年度のシラバスには、概要と目標が次のように記載されている。

> コロキウムは「21 世紀に必要とされる教養とはなにか」をテーマに考えだされた本校独自の学校設定科目である。授業形式は、授業者と選択者の対話による学びの場の形成をめざしている。授業者と選択者の 1 年間を通しての活動が、教科などの枠を越えた自由な実践へとつながり展開されていくことを期待する。本年は担当教員によって下記の目標に基づいた 8 講座が展開される。
>
> ■コロキウムの目標
>
> 1）21 世紀に求められる Citizenship（市民的素養）の育成
>
> 2）“学問の根底にある精神”を中等教育において学ぶ

また、生徒が受講講座を選択する際の説明資料には、講座の概要を次のように記した。

数学と聞いて、何を思い浮かべるだろう？　「好き」「嫌い」「何の役に立つのだろう」「答えが 1 つに決まるのが楽しい」等々。各人の感じ方はいろいろあるけれど、数学に対してよく言われることだ。この講座では、数学が好きな人も嫌いな人も、ちょっと視点を変えて数学とつきあって欲しい。そして、これまでの数学に対する感覚や考え方が変化し、数学の新たな側面を発見するような学習ができることをねらいとする。

講座の後半では、数学に関して興味関心を持った領域について、自分で問いを立て、その問いについて探究し、様々な方法でまとめて発表する。このような活動を通じて、教科の授業で学習する数学とは違う視点を獲得し、人類の文化遺産としての数学を感得することを目指す講座である。

「文化としての数学を」のカリキュラムは、次ページを見ていただきたい。特殊相対性理論の前半部分は、生徒 3 人のグループが、自分たちで学んだ内容を説明するゼミ形式で行った。後半部分は時間の関係で実践できなかったが、引き続いて自学する生徒もいた。

また、終盤に各人が興味・関心にしたがって自分でテーマを設定し、探究活動を行った。その結果を論文としてまとめたものが、「LADy SCIENCE BOOKLET 2『文化としての数学を　生徒論文集』」である。

コロキウムでの学習活動を通じて、出来上がった教科書の数学とは違う文化としての数学を感じ、味わい、理解してくれたとすれば幸いである。

2015 年 3 月 27 日

奈良女子大学　全学共通教授

吉田信也

■目次

■2014 年度　コロキウム　講座「文化としての数学を」カリキュラム

コロキウム「文化としての数学を」		
月	日	内容
4	18	π の歴史
	25	π の歴史
5	2	π を求める
	9	π を求める
	23	確率統計
6	6	確率統計
	13	確率統計
	20	確率統計
7	4	暗号の歴史
	11	暗号の歴史
9	12	暗号の歴史
	26	科学の言葉としての数学「特殊相対性理論」
10	17	科学の言葉としての数学「特殊相対性理論」（ゼミ形式）
	31	科学の言葉としての数学「特殊相対性理論」（ゼミ形式）
11	7	科学の言葉としての数学「特殊相対性理論」（ゼミ形式）
	14	科学の言葉としての数学「特殊相対性理論」（ゼミ形式）
	28	個人・グループでの探究活動
12	12	個人・グループでの探究活動
1	9	個人・グループでの探究活動
	16	個人・グループでの探究活動
	30	個人・グループでの探究活動
2	6	研究発表会
	13	研究発表会
	20	研究発表会
	27	年間のまとめ

第 1 章　数学と歴史

「πの歴史は，人類の歴史をうつしだすちいさな鏡である。それは，シラクサのアルキメデスの物語である。この人のπの計算法は1900年にもわたって，いささかも変えられなかった。またそれは，クリーヴランドの実業家の物語でもある。この人は1931年に，πが正確に $\frac{256}{81}$ に等しいという大発見をし，それをひろめるために本を書いた。ところがこの値は，4000年もの昔エジプト人が使っていたものなのだ。さらにそれは，紀元前3世紀のアレクサンドリア大学の物語であり，科学書に火をつけて焼き払うという愚かなことをやった中世の司祭や十字軍の物語でもある。彼らにいわせると書物の内容が悪魔のしわざだという理由からであった。」

『πの歴史』ペートル・ベックマン(ちくま学芸文庫)

このように，よく知られた円周率πについても，長い歴史がある。紀元前からπの値については調べられていたし，πに興味を持って研究する人は現在でも絶えない。ここでは，πだけではなく，その他の数学的事項についても，歴史的な側面から迫っていきたい。

ところで，右の絵画を見たことはあるだろうか？　ルネッサンス期イタリアの画家ラファエロの描いた「アテナイの学堂」である。ここには，ギリシャの哲学者・科学者のほとんどが描かれていると言われているが，諸説ある。今後，登場するであろうプラトン，アリストテレス，ユークリッドがどこにいるか，探してみよう。

§1　円周率を求める 1

『πの歴史』にあるように，円周率πについての計算は古くから行われていた。現在ではコンピュータと計算する方法(アルゴリズム)の発達により，2014年現在，小数点以下13.3兆桁!!まで計算されている。ちなみに，小数点以下100万桁までは，次のようになっている。

3. 1415926535 8979323846 2643383279 5028841971 6939937510 5820974944 5923078164 0628620899 8628034825 3421170679
8214808651 3282306647 0938446095 5058223172 5359408128 4811174502 8410270193 8521105559 6446229489 5493038196
4428810975 6659334461 2847564823 3786783165 2712019091 4564856692 3460348610 4543266482 1339360726 0249141273
……
0315614033 3212728491 9441843715 0696552087 5424505989 5678796130 3311646283 9963464604 2209010610 5779458151

また，古代からの主に円周率に関するできごとを簡単にまとめると，次のようになる。

年代	できごと
BC2000頃？	・バビロニア人，$\pi=3+\frac{1}{8}$ を使う ・エジプト人，$\pi=\left(\frac{16}{9}\right)^2=3.165$を使う ・粘土板文献『プリンプトン322』の「ピタゴラスの三つ組」(メソポタミア文明)
BC1850頃	・『モスクワ・パピルス』(エジプト文明)
BC1650頃	・『リンド・パピルス』(エジプト文明)
BC12世紀	・中国人，$\pi=3$を使う
BC4世紀頃？	・通約不可能性の発見
BC3世紀頃	・ユークリッド『原論』 ・アルキメデス, $3+\frac{10}{71}<\pi<\frac{31}{7}$ を確立
BC186	・『算数書』(中国)
BC1世紀～AD1世紀？	・『九章算術』(中国)
3世紀頃	・ディオファントス『算術(Arithmetica)』 ・『孫子算経』中国式剰余定理
263	・劉徽による『九章算術』の注釈，$\pi=\frac{157}{50}=3.14$を使う
5世紀	・祖沖之，$3.1415926<\pi<3.1415927$を確定
8世紀	・遅くともこの頃までに，10進位取り記数法がインドで成立
9世紀	・アル＝フワーリズミ『アルジャブルとアルムカーバラの計算の書』
1202	・フィボナッチ『算盤の書』
1600前後	・ファン・ケーレンによる小数点以下35桁までのπの計算
1674頃	・ライプニッツによる「$\frac{\pi}{4}$ 公式」
1722	・建部賢弘『綴術算経』小数点以下41桁までのπの計算
1739	・松永良弼『方円算経』小数点以下49桁までのπの計算
1882	・リンデマンによるπが超越数(※)であることの証明

(※)　超越数とは，代数方程式　$x^n+a_{n-1}x^{n-1}+\cdots+a_0=0$　($n\geqq 1$，a_kは有理数)の解とはならない複素数のことである。

人間は，道具を使い出し，大きさと数の概念を獲得し，測定を通じて量の間の関係を認識するようになってきた。しかし，これらが具体的にどのようになされてきたかについては，よくわかっていない。BC2000年ごろまでは情況証拠ばかりである。その中で，きちんとした証拠を元に，人類はBC2000年ごろまでに円周率πの重要さを知り，その値も計算していたことがわかっている。

いったい，そんな昔にどのようにして人類はそこまで到達できたのか。まず，人類は初めは2つのものをかぞえることを学び，もっと大きな数をかぞえるまでは長い時間がかかったようだ。その証拠の1つである，人間の言語の中に残されているものは非常に興味深い。

・ボヘミヤ語：中世まで2種類の複数(2つのものと，2つより多いもの)が使用されていた
・フィンランドではいまも2種類の複数が使用されている
・ゲルマン系の言語では，2(two)と1/2(half)にはなんの関係もない
・ラテン系，スラブ系の言語も同様
・しかし，すべてのヨーロッパの言語では，

3と $\frac{1}{3}$ ，4と $\frac{1}{4}$ などは関係を持っている　(*)

このことから，人類が比例や逆数の概念を認識したのは，2以上の数を知ってから後のことだと考えられる。

［問1］上記の(*)について，具体的に述べよ。

3：third　$\longleftrightarrow$　$\frac{1}{3}$：one third

4：fourth　$\longleftrightarrow$　$\frac{1}{4}$：one fourth

このようにして，2以上の数を知った人類の次のステップは，いろいろな数の間の関係を見出すことであった。大きさ重さの関係，速さと距離の関係などを，定性的な理解から定量的な理解へ進めながら，数の間の関係を獲得してきた。

そのいちばん基本の形は，比例の関係であっただろう。つまり，

1組の量があって，片方が2倍・3倍・4倍となれば，他方も2倍・3倍・4倍となる

という関係である。

このことから，比例定数が存在することを認識し，その1つとして，

円周率π＝円周/直径

を考えたのであろう。

BC2000年には，人類はすでに円周率という定数が存在することを認識するとともに，その近似値も発見していた。

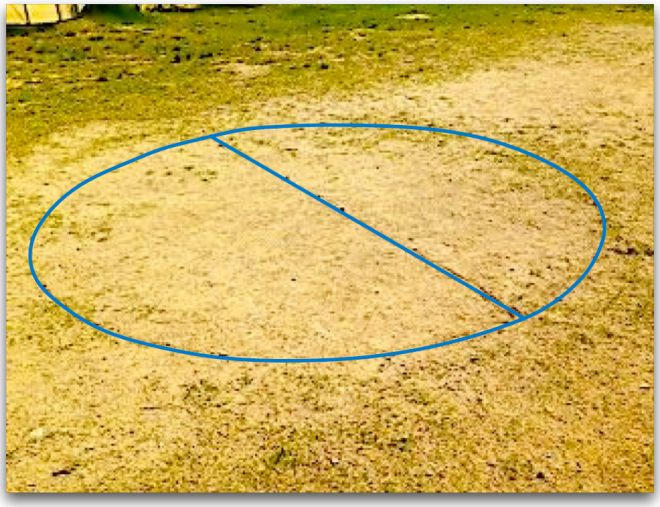
バビロニア人：$\pi=3\frac{1}{8}$

エジプト人：$\pi=4\times(8/9)^2$

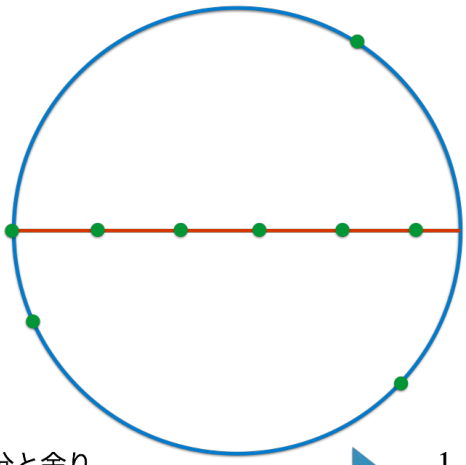
さて，古代の人達はどのようにしてこれらの値を知ったのだろう？

［問2］BC3000年のエジプトでは，測量をするのに杭と縄を使っていた。君たちはBC3000年の時代の若者として，円周率をどのようにして求めればよいか考えよう。

・校庭に出て，棒とトラロープでπを求める



・実験の結果



直径3つ分と余り
余りで直径を測ると5つとちょっと

$3\frac{1}{6}<\pi<3\frac{1}{5}$

・これを繰り返すと，πの値はいくらでも厳密にできるか？　きちんと測りきれるか？
→測りきれたらπは有限小数となる。しかし，πは超越数であることが知られている。

§2　円周率を求める 2

引き続いて，円について考えよう。半径rの円の面積をSとすると，

$S=\pi r^2$　・・・(☆)

であることは，君たちはすでに事実として知っている。そして，5000年前の古代の人たちも円の面積が(☆)であることは，知っていたと推測される。

この時代は，長方形の面積が，(たて)×(よこ)で求められることを知っていた。そこで，平行四辺形の面積の求め方も知っていただろう。

［問3］古代の人々が，どのような方法で平行四辺形の面積を求めたかを，推測せよ。

・平行四辺形を長方形に変形して求めた

そして，たぶん同様な考え方で円の面積を求めたのだろう。

［問4］古代の人々が，どのような方法で円の面積を求めたかを，推測せよ。

・円を細かい扇形に分割し，それを並べ替えて平行四辺形を作って求めた

→底辺が πr，高さrの平行四辺形ができるので，$S=\pi r\cdot r=\pi r^2$

現在では，積分法で円の面積が(☆)であることは，数学的に求められる。

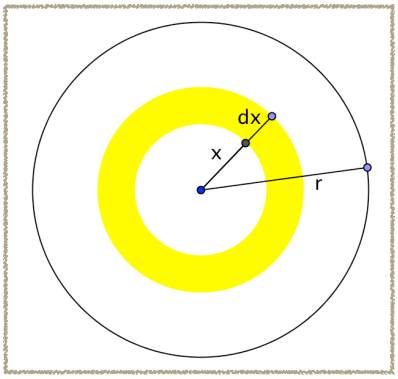
簡単に説明すると，次のようになる。

［積分法による円の面積の求め方の一例］

右図において，網目の微小円環部分の面積は，微小な幅をdxとすると，

$2\pi x\times dx=2\pi x dx$

となる。この微小円環の面積を連続的に足し合わせると，円の面積となるので，求める円の面積は，



$$\int_0^r 2\pi x\,dx=2\pi\int_0^r x\,dx=2\pi\left[\frac{1}{2}x^2\right]_0^r=\pi r^2$$

このように強力な微積分法は，イギリスのニュートン(1643−1727)とドイツのライプニッツ(1646−1716)の2人の天才によって，独立に発見された。

ニュートンは，運動力学や天文学などの当時の自然科学のテーマにおける基本原理を，数学で表現しようとして，微分積分学を創成したのである。その結果，リンゴから惑星まで(地上から天上まで)の運動の背後に潜む原理を，統一的に説明することに成功したのである。その偉業を讃えて，詩人アレキサンダー・ポープは，ニュートンの墓碑銘として次のように記している。

自然と自然法則は闇に隠れていた。神は言われた。

「ニュートンあれ。」こうして光があった。

それに対してライプニッツは，哲学者であり自然学者であり神学者でもあった。そして，形式的な記号の組み合わせによる普遍数学の夢を持っていた中での，微分積分学の発見であった。ライプニッツの考案した記号は，現在でも利用されている素晴らしいものである。

円周率πの値を理論的に考えて計算した人たちは，昔からたくさんいる。

紀元前3世紀：	古代ギリシャのアルキメデス	$3\frac{10}{71}<\pi<3\frac{1}{7}$
263年：	中国の劉徽	$\pi=\frac{157}{50}=3.14$
5世紀：	中国の祖沖之	$3.1415926<\pi<3.1415927$

ここでは，古代ギリシャの天才アルキメデスが考えた方法を追体験しよう。ただし，私たちは現代的な記法を用いて計算する。アルキメデスの時代と，アルキメデス自身の計算については，次のことに注意しておこう。

・古代ギリシャでは，分数の記号はなく，すべては比の形で表されていた
・古代ギリシャでは，位取り記数法がなかったので，計算は大変面倒であっただろう
・小数もほとんど利用されていなかったので，アルキメデスは計算に苦労しただろう
・アルキメデスの計算のいちばん重要な部分は，平方根をとるところであるが，アルキメデス自身がどのように計算したのかはよくわかっていない

さて，アルキメデスの方法で円周率πの値を計算しよう。アルキメデスの考え方は，

[1]　円周の長さを，円に内接する正n角形と，外接する正n角形の周囲の長さで近似する

[2]　n＝6から始めて，n＝12，24，48，96として，πの値を評価する

というものであり，いろいろな時代に，いろいろな人たちが用いた考え方である。

ここでは，

円の半径を1
円に内接する正n角形の1辺の長さをa_n
円に外接する正n角形の1辺の長さをb_n

とおいて，漸化式を作って考える。

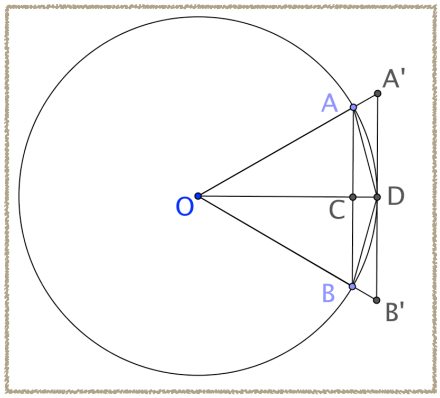
一般的に考えることのよさと漸化式の有用性

を感じられるだろう。

右図において，

△OABは内接正n角形の1つの三角形
△OA' B'は外接正n角形の1つの三角形
点Cは辺ABの中点で，OCと円の交点をD
辺A' B'は点Dにおける接線

とする。



△OAC～△OA’Dであるから，

$$\frac{AC}{A'D}=\frac{OC}{OD}$$

ここで，

$$\mathrm{OD}=1,\ \mathrm{AC}=\frac{1}{2}a_n,\quad \mathrm{A'D}=\frac{1}{2}b_n,$$

より，

$$\mathrm{OC}=\frac{a_n}{b_n}\cdots①$$

△OACは直角三角形だから，三平方の定理より，

$$\mathrm{OC}=\sqrt{OA^2-AC^2}=\sqrt{1-\frac{1}{4}a_n{}^2}=\frac{1}{2}\sqrt{4-a_n{}^2}\cdots②$$

①，②より，

$$\frac{a_n}{b_n}=\frac{1}{2}\sqrt{4-a_n{}^2}$$

よって，

$$b_n=\frac{2a_n}{\sqrt{4-a_n{}^2}}\cdots③$$

△ACDは直角三角形だから，三平方の定理より，

$$\mathrm{AD}^2=\mathrm{AC}^2+\mathrm{CD}^2=\frac{1}{4}a_n{}^2+(1-\mathrm{OC})^2$$

$$=\frac{1}{4}a_n{}^2+(1-\frac{1}{2}\sqrt{4-a_n{}^2})^2$$

$$=2-\sqrt{4-a_n{}^2}$$

$\mathrm{AD}=a_{2n}$より，

$$a_{2n}=\sqrt{2-\sqrt{4-a_n{}^2}}\cdots④$$

［問5］漸化式③，④を利用して，内接正96角形，外接正96角形の周囲の長さを計算することにより，円周率πの値を評価せよ。

【計算】必要なら，電卓やコンピュータを使ってもよい。

・WolframAlphaの利用の仕方を指導

→http://www.wolframalpha.com/

数式処理システムMathematicaによる計算を行うと，次のようになる。

$$a[n\_] := \sqrt{2 - \sqrt{4 - a\left[\frac{n}{2}\right]^2}} \; ; \; a[6] := 1$$

$$a[12]$$

$$\sqrt{2 - \sqrt{3}}$$

$$a[24]$$

$$\sqrt{2 - \sqrt{2 + \sqrt{3}}}$$

$$a[48]$$

$$\sqrt{2 - \sqrt{2 + \sqrt{2 + \sqrt{3}}}}$$

$$a[96]$$

$$\sqrt{2 - \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{3}}}}}$$

$$b[n\_] := \frac{2\, a[n]}{\sqrt{4 - a[n]^2}}$$

$$b[6]$$

$$\frac{2}{\sqrt{3}}$$

$$b[12]$$

$$2\sqrt{\frac{2 - \sqrt{3}}{2 + \sqrt{3}}}$$

$$b[24]$$

$$2\sqrt{\frac{2 - \sqrt{2 + \sqrt{3}}}{2 + \sqrt{2 + \sqrt{3}}}}$$

$$b[48]$$

$$2\sqrt{\frac{2 - \sqrt{2 + \sqrt{2 + \sqrt{3}}}}{2 + \sqrt{2 + \sqrt{2 + \sqrt{3}}}}}$$

$$b[96]$$

$$2\sqrt{\frac{2 - \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{3}}}}}{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{3}}}}}}$$

$$\text{Table}\left[\left\{\frac{N\left[a\left[6 \times 2^{n-1}\right]\right] \times 6 \times 2^{n-1}}{2}, \frac{N\left[b\left[6 \times 2^{n-1}\right]\right] \times 6 \times 2^{n-1}}{2}\right\}, \{n, 1, 5\}\right]$$

```
{{3., 3.4641}, {3.10583, 3.21539}, {3.13263, 3.15966}, {3.13935, 3.14609}, {3.14103, 3.14271}}
```

先に述べたように，アルキメスは比で計算していた。円周率の計算では，例えば，

$$\sqrt{3} \fallingdotseq \frac{265}{153}$$

と近似した。ちなみに，

$$\sqrt{3} \fallingdotseq 1.73205,\quad \frac{265}{153} \fallingdotseq 1.73203$$

であるから，かなりよい近似値であることがわかる。

また，正12角形の計算では，

$$\sqrt{349450} : 153 \fallingdotseq 591\frac{1}{8}$$

と近似している。

ちなみに，Mathematicaで計算すると，

$$\sqrt{349450} \fallingdotseq 591.143,\quad 591\frac{1}{8} \fallingdotseq 591.125$$

である。

さらに，正96角形の計算では，10進法で10桁の数の平方根を含んでいる！

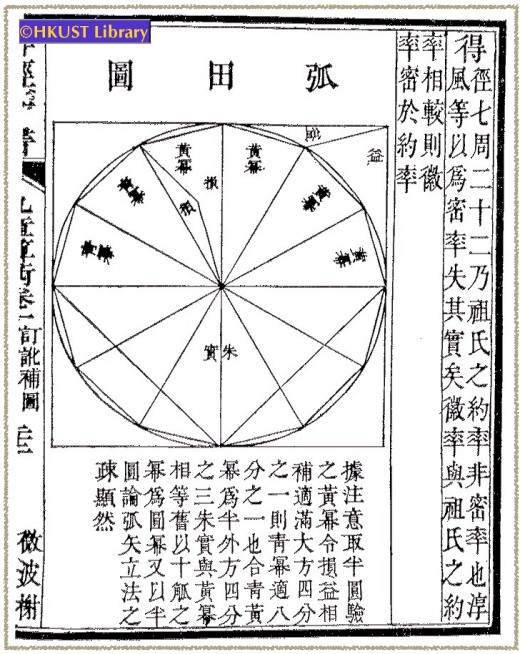
アルキメデスの方法で円周率を計算する際には，平方根の処理が常に問題となる。これらの平方根の計算を，絶えず上限と下限に対して，より小さく，より大きくなるように注意をはらいながら行ったのである。どのような方法で，この驚異的な精度の平方根の計算を行ったのかは，超人アルキメデスが現代に残した謎の1つである。

ここまで，アルキメデスを中心に考えてきた。現代の数学の様子からは，ユークリッドやアルキメデス等の古代ギリシャの数学が源となっていて，他の国や地方では数学が発展していなかったような印象を受けるかもしれない。しかし実は，地球の中緯度のベルト地帯である，エジプト，ペルシャ，インド，中国と農業革命が起こったところには，豊かな数学が花開いていたのである。

例えば，中国の劉徽は右図のような方法をとっていた(264年)ことが，18世紀の文献に残っている。中国人は，古代人の中で非常に初期から10進法を使った唯一の民族である。そして，数字0に相当するものを発見して利用していた。そうでないと，5世紀に祖沖之が

$$3.1415926 < \pi < 3.1415927$$

の精度で計算できなかったであろう。この精度は，ヨーロッパでは 16 世紀になるまで到達できなかったものである。



第 2 章　数学と社会生活

数学は社会で役に立っているのか？

数学はどこに利用されているのか？

このような問い・疑問を持つ人は多いだろう。実際に，ずいぶんと以前の話であるが，有名な女性作家であるSAが，次の趣旨のことを言った。

私は2次方程式もろくにできないけど，65歳になる今日まで全然不自由しなかった

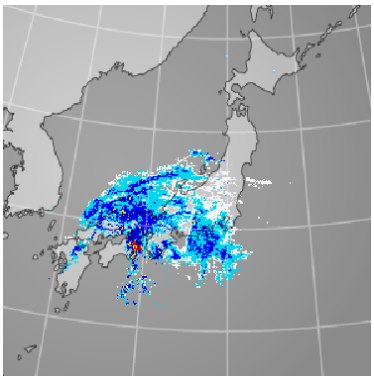
これを家庭で聞いた彼女の夫の，これも高名な作家であるMSが，自身が会長を務める教育課程審議会で紹介したところ，「そうだ，その通り」との賛同の声が大きく，結局そこで審議されていた中学校数学の学習指導要領から2次方程式の解の公式が消えて，高等学校で学習することになってしまった。「ゆとり教育」と呼ばれる学習指導要領の時代である。幸いにして，現在の学習指導要領では中学校で学習するように戻っているが，

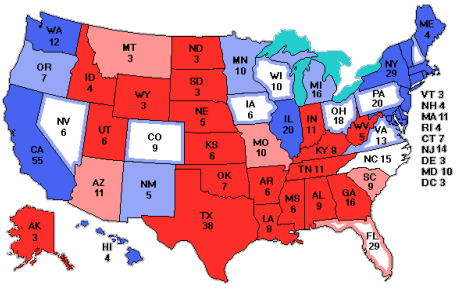
数学が役に立つかどうかを短絡的に，文化というものを理解せずに判断

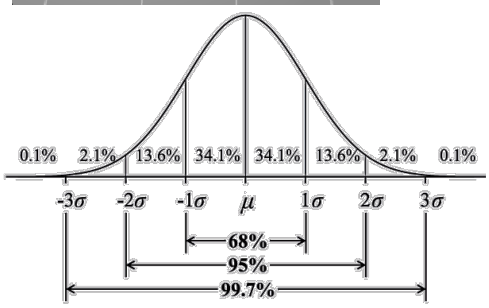
すると，以上のような哀しい結果になってしまう。

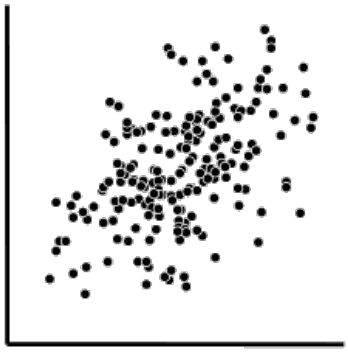
しかしながら，大部分の学校において，大学入試合格をゴールとするような教育として「学校数学」が教えられてきたことは，否めない事実である。文化としての数学が，社会生活において大いに役立っている，人間が市民として賢く生きていくための基盤となっていることが実感できる数学を，学校で学ばなければならないと考える。

ここでは，天気予報等で身近で実生活と密接に関係している確率・統計で楽しみ，18世紀のドイツの天才数学者ガウスが数学の女王と呼んだ整数論が，現代生活の最先端で活用されていることを学習しよう。









§1　確率・統計の思考で賢く生きよう

私たちの日常生活では，偶然に支配されるために，確率を用いて表される出来事がたくさんある。例えば，次のように放送や新聞発表がなされる。

天気予報で「明日の降水確率は40%」

選挙で「ブッシュがケリーを47%対45%でリードしている，誤差の範囲は±2.9%」

もしも神様がいるならば，明日に雨が降るかどうかはわかるはずであり，選挙も誰が当選するかは明らかなはずである。しかしそうではないので，私たちは日常生活の曖昧さや不確実性を確率や統計で表現しているのである。私たちの生活には，確率・統計はなくてはならないものになっているので，これらをきちんと理解して生きていきたいものである。

では，常識にとらわれずに，次の問いを自分でじっくりと考えてみよう。

［問1］A君は、家族で千葉のディズニーランドに出かけて2日間，思い切り遊んだ。そのとき驚いたのは，何千人の見知らぬ人たちの中で，従兄弟のB君の家族とばったり出会ったことだった。さて，これはどれくらい驚くべきことなのだろう？

・日本の人口は1おく3千万人だから，B君と合う確率は $\frac{1}{130000000}$ と凄く小さい

・しかし，2日間で少なくとも2000人とは出会い，そのうちの誰がB君でもおかしくはない

→確率は，$\frac{1}{130000000}\times 2000=\frac{1}{65000}$

・ばったり出会って驚く相手は，500人はいるだろう

→確率は，$\frac{1}{65000}\times 500=\frac{1}{130}$

・これはまだ小さい確率だが，一生のうちに彼方此方に出かけることを考えると，それほど驚くべきことでもない

［問2］コップ1杯の水を，大阪の南港の海に注いだ。その水は海流に運ばれたり，蒸発したり，雨になって降り注いだりして，全世界に広がっていき，世界中の水と混じりあう。さて，5年後に貴方が日本の裏側のブラジルの海に行って，コップ1杯の水をすくい取るとき，ブラジルのコップの中に，日本のコップに入っていた水分子は含まれているだろうか？　含まれているとすれば，その分子の個数は何個で，どれくらい珍しいことなのだろう？

・水H_2Oは1molだと18g であり，1g の水は1cm^3なので，コップ1杯の容量を180cm^3とすると，その中には10mol 個の水分子が含まれる

・地球の海水量は，$1.4\times 10^9 km^3=1.4\times 10^{24} cm^3$

・コップ1杯に含まれる元の水の分子の数は，

$$\frac{6.02\times 10^{24}\times 180}{1.4\times 10^{24}}=774個$$

［問3］C君のクラスは40人だが，調べたところ同じ誕生日の人がいたのでびっくりした。さて，これはどれくらい驚くべきことなのだろう？

・同じ誕生日の人がいる確率は，$1-\frac{365!}{365^{40}(365-40)!}$ ＝0.8912←WolframAlphaで計算させる

→そんなに驚くべきことではない

［問4］全日本瞑想協会の年会費は100万円であり，瞑想家の会長の指導で会員は1日に2時間の瞑想を行う。会員全員が健康診断を行ったところ，一般の人と比べて血圧は低く，体脂肪は少なく，筋肉量は多く，コレステロール値は低いなど，会員の健康状態は非常によいことが判明した。そこで，Dさんは健康になりたいので全日本瞑想協会に入ろうと考えた。貴方はこれについてどう考えますか？

・年会費100万円を払える人は，もともと健康な人が多い

・相関と因果律(原因と結果)の混同

［問5］右の表は，2011年のいくつかの国別の殺人発生件数である。E君はこの表を見て，殺人に関して最も危険な国はアメリカで，最も安全な国はエストニアであると言った。貴方は，E君の意見についてどう考えますか？

・割合(例：人口10万人あたり)を調べなければならない

UNODC
United Nations Office on Drugs and Crime

Country/territory	2011年
Canada	529
United States of America	14,661
Japan	442
Australia	244
Estonia	65
Lithuania	211
United Kingdom	653
Germany	662
France	743

［問6］ある投資では，確率0.5で投入資金が4倍になり，確率0.5で投入資金をすべて失ってしまう。F君はこの投資に100万円を一発で投入し，Gさんは10万円ずつ10回に分けて投入する。さて，F君とGさんでは，どちらの方が儲けを期待できるか？

・F君：50%の確率で100万円を失う，これは十分にあり得る

・G君：100万円を失う確率は，$\left(\frac{1}{2}\right)^{10}$ ≒0.001で，ほとんど起こらない

［問 7］3 つのドアがあって，1 つのドアの後ろには車があり，司会者は車のあるドアを知っている。貴方は 1 つのドアを選び，司会者は残った 2 つのドアのうちの 1 つ(車のないドア)を開ける。ここで，貴方にチャンスが与えられる。最初のドアのままでもいいし，まだ開いていないドアを選択しなおしてもよい。最終的に選んだドアの後ろに車があれば貴方のものになり，なければ負けとなる。さて，貴方はドアを変えた方がいいのか，変えない方がいいのか。車をもらえる確率は，どちらが高い？

・直観で答える

・グループに分かれて実験する

→実験結果は，ドアを変更するほうが確率が高くなりことを示す

→実験結果の例：

	ドアを変更した					ドアを変更しない				
メンバー	赤木･延江	西尾･田中	竹割･早崎	上松･北山	合計	赤木･延江	西尾･田中	竹割･早崎	上松･北山	合計
実験回数	22	26	19	34	101	18	17	20	33	88
○あたり	15	16	7	19	57	8	12	5	12	37
×はずれ	7	10	12	15	44	10	5	15	21	51
○の確率	0.564					0.420				

［問8］上の実験結果から，ドアを変更したほうが当たる確率が高いと予想できるだろう。この予想を，数学的に考えてみよう。

(1)　貴方の考え

(2)　実験のペアで議論した内容・結果

(3)　全員でのシェア

問 7(モンティ・ホール問題)について， 貴方がドア A を選んだとして， まとめておこう。

［説明1］

このゲームの初め，貴方は車がどこにあるのかは知らなかったので，ドアAは完全にランダムに選んだから，ドアAに車がある確率は$\frac{1}{3}$である。

次に，司会者が開けるドアは車のないドアだとわかっているので，司会者がドアを開けて車がなかっても，それは当然のことである。つまり，司会者がドアを開けても，貴方が最初に選択したドアが当たりかどうかという確率にはいっさい影響はないので，ドアAに車がある確率は$\frac{1}{3}$のままである。すると，ドアAに車がある確率が$\frac{1}{3}$なので，残ったドアに車がある確率は$\frac{2}{3}$となる。ドアを変えたほうが，確率は2倍になる！

［説明2］

司会者は, 車のないドアをランダムに開けるので, コインを投げて開けるドアを決めるとする。開けるべきドアが1つしかないときも，コインを投げて決める。すると，考えられる場合は次の表のようになる。

貴方の選択	車のありか	コイン	司会者の選択
ドアA	ドアA	表	ドアB
ドアA	ドアA	裏	ドアC
ドアA	ドアB	表	ドアC
ドアA	ドアB	裏	ドアC
ドアA	ドアC	表	ドアB
ドアA	ドアC	裏	ドアB

ゆえに，ドアAのまま変更しないと当たるのは2通り，変更すると当たるのは4通りなので，ドアを変更したほうが確率は2倍となる！

［説明3］

ドアを変更したほうが当たる確率が大きくなるのは，次の極端な場合を考えれば，納得できるだろう。

ドアが100枚あって，司会者は車のないドア98枚を開け放す。

納得できた？

・ドアAで当たる確率は$\frac{1}{100}$，残りのドアで当たる確率は$\frac{99}{100}$

確率・統計は，医学の研究でも利用される。

例えば，確率50%で死に至る病気Sがあったとする。ある製薬会社が新薬を開発し，この薬で病気Sの致死率を下げられると主張している。このようなとき，検証のために臨床試験が行われる。

［問9］病気Sの5人の患者に新薬を投与して臨床試験をした結果，5人全員が助かった。この結果は，新薬の有効性を証明しているだろうか？　有効だとするなら，その根拠をどこに求めるのだろう？

［問10］あるガンの罹患率は0.5%である。このガンの検診方法があり，的中率は95%である。貴方がこの検診を受けてガン陽性であるとの結果が出たとする。貴方は，どれくらい心配するだろう？

世の中の統計学者には，フィッシャー派(頻度論派)とベイズ派(条件確率派)がいる。

フィッシャー派は，p値(有意確率)や誤差の範囲，「20回に19回まで」といった判断で，統計的な推論を行う。それに対して，ベイズ派はあらゆる不確定要素については，条件確率を求めなければならないと信じている。

問9について，両方の立場からまとめてみよう。

■フィッシャー派

p値を求める事から始める。すなわち，全くの偶然から5人全員が回復した確率を求める。

$$\left(\frac{1}{2}\right)^5 = \frac{1}{32} \fallingdotseq 0.031 = 3.1\%$$

このp値は5%より小さいので，5人全員が全くの偶然から回復することはありえない，すなわち，この新薬は有効であると判断する。

■ベイズ派

まず，新薬の効き目に「事前確率]」を割り当てる。私たちには，この新薬が有効かどうかはわからないし，公平に判断したいので，次のように考える。

A：新薬が有効であり，全員助かる　　その確率P(A)＝0.5

B：新薬は無効であり，生存率は50%のまま　　その確率P(B)＝0.5

このもとで，5人の患者全員が助かったときの新薬が有効である確率，条件付き確率を求めるのである。

X：5人の患者全員が助かる

とすると，求める確率は，

$$P_X(A) = \frac{P(X \cap A)}{P(X)}$$

である。ここで，

$$P(X\cap A)=\frac{1}{2}$$

$$P(X)=P(X\cap A)+P(X\cap B)$$

$$=\frac{1}{2}+\frac{1}{2}\cdot\left(\frac{1}{2}\right)^5=\frac{2^5+1}{2^6}$$

よって,

$$P_X(A)=\frac{2^6}{2^5+1}\cdot\frac{1}{2}=\frac{32}{33}\fallingdotseq 0.9697=96.97\%$$

つまり, この新薬が有効である事後確率が0.9697, 無効である確率が0.00303であると断言する。

［問10］フィッシャー派とベイズ派は，お互いに批判し合い論争を続けてきた。どの点に対して，「攻撃」が行われたのか考えてみよう。

・5%に意味があるの？　誤差の範囲，p値に意味はない，実際のデータがないと何も言えない，論理的につじつまが合わない

・実験が始まらないうちから結果を問う，事前確率に根拠はあるのか？

［問11］1枚のコインがあり，本物か偽物のどちらかである。本物の表の出る確率は0.5，偽物の表の出る確率は0.6である。このコインを2回続けて投げたら，2回とも表であった。コインが本物か偽物かを，ベイズ派の考えで推定しよう。

(1)　本物である確率と偽物である確率(事前確率)をともに0.5であるとして，コインが偽物である推定値(事後確率)を求めよ。

(2)　1回目に表が出たことから，偽物である推定値(確率)を変更し，そのもとで2回目に表が出た結果から，コインが偽物である推定値(事後確率)を求めよ。

(3)　以上から，どのようなことがわかるか。

(1)　偽物の確率は，$\frac{1}{2}\times\left(\frac{6}{10}\right)^2$，本物の確率は，$\frac{1}{2}\times\left(\frac{1}{2}\right)^2$ より，偽物：本物＝$\frac{36}{61}$：$\frac{25}{61}$

(2)　1回目に表が出る確率は，偽物：$\frac{1}{2}\times\frac{6}{10}$，本物：$\frac{1}{2}\times\frac{1}{2}$ より，偽物：本物＝$\frac{6}{11}$：$\frac{5}{11}$

よって，2回目は，偽物：本物＝6：5と推定値を変更する。

2回目に表が出る確率は，偽物：$\frac{6}{11}\times\frac{6}{10}$，本物：$\frac{5}{11}\times\frac{1}{2}$ より，偽物：本物＝$\frac{36}{110}$：$\frac{25}{110}$

(3)　偽物：本物＝$\frac{36}{61}$：$\frac{25}{61}$＝$\frac{36}{110}$：$\frac{25}{110}$ より，データ2つでアップデートした(1)の事後確率と，データ1つで推定値をアップデートした(2)の結果は同じである。

→　現在の推定値を，新しいデータだけから改定すればよい

→ベイズ推定は，FAXのノイズ除去，MSのヘルプ，ネットショッピングの問合せ等に利用

§2数学のおかげで安心してネット利用

1. 暗号の歴史

現在，多くの人々がインターネット上でショッピングを行っているが，通常は情報を盗みとられることなく安心して利用されている。これは，ショッピング等における情報が暗号化されているからである。ここでは，暗号の歴史にも触れながら，暗号化に数学がどのように活用されているかを学習しよう。

暗号は大昔から利用されているが，軍事目的に利用された記録として最も古い文献は，ユリウス・カエサルの『ガリア戦記』である。カエサルは，アルファベットの各文字を，それよりも3つ後ろの文字で置き換えて暗号を作成した。このような，文字をずらして作成する暗号は，カエサル暗号またはシーザー暗号と呼ばれる。カエサル暗号では，ずらす文字数は1文字から25文字まで考えられるので，25種類の暗号ができることになる。

［問1］カエサル暗号のような文字を置き換える暗号において，アルファベットをどのように並べ替えてもよいとすれば(一般的な換字式暗号)，作れる暗号は何種類か。式とその計算結果を求めよ。計算では，コンピュータを利用してもよい(利用しないと計算できない)。

・$26!-1=403291461126605635584000000-1\fallingdotseq 4\times 10^{26}$

暗号は，「アルゴリズム」と「鍵」によって構成されている。

アルゴリズム：暗号化の大まかな方針

鍵：厳密に1つの方法を指定すること

■カエサル暗号

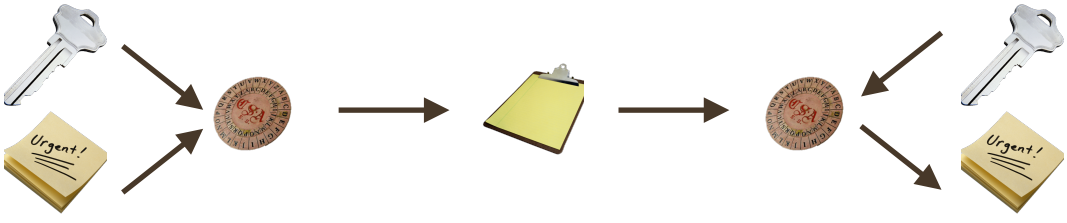
アルゴリズム：アルファベットを置き換える

鍵：アルファベットを何文字ずらすか(候補は25通りしかない)

■問1の暗号(一般的な換字式の暗号)

アルゴリズム：アルファベットを置き換える

鍵：アルファベットをどう置き換えるか(候補は　4×10^{26}　通りもある！)



平文　　アルゴリズム　　暗号文　　アルゴリズム　　平文

以上のことからもわかるように，暗号システムの安全性は，暗号化アルゴリズムを秘密にすることには関係なく，鍵の秘密を守ることにかかっている。

一般的な換字式暗号は，その鍵の種類の多さから解読は不可能なように思える。実際，スパイが毎秒1つの鍵をチェックするとして，鍵をすべてチェックし終えるには宇宙の年齢の約10億倍もの時間がかかる。しかし，イスラム文明のアラビア人たちは，このような暗号を解読する方法を発見した。暗号解読法が生まれるためには，数学，統計学，言語学などの学問が発達しなければならないが，8世紀以降のイスラム文明はそのことが可能となるほど高度なものだったのである。

［問2］アラビア人が発見した，換字式暗号の解読法はどのような考え方であったかを，アルファベットについて説明せよ。

アラビア人の暗号解読法に関する最古の記述は，9世紀の科学者でありアラブの哲学者として知られる，アブー・ユースフ・ヤアクーブ・イブン・イスハーク・イブン・アッサバーフ・イブン・ウムラーン・イブン・イスマイール・アル＝キンディーによるものである。その概要をアルファベットで説明すると，次のようになる。

1. ある程度の長さを持つ普通の英文(平文)における，アルファベットの出現頻度を調べる

文字	出現頻度(%)	文字	出現頻度(%)	文字	出現頻度(%)
a	8.2	j	0.2	s	6.3
b	1.5	k	0.8	t	9.1
c	2.8	l	4.0	u	2.8
d	4.3	m	2.4	v	1.0
e	12.7	n	6.7	w	2.4
f	2.2	o	7.5	x	0.2
g	2.0	p	1.9	y	2.0
h	6.1	q	0.1	z	0.1
i	7.0	r	6.0		

2. 暗号文におけるアルファベットの出現頻度を調べる
3. 上記2つの出現頻度を見て，出現頻度の高い文字から置き換えの候補を絞る
4. それらの文字の隣に現れる文字に注目し，もし母音なら前後には様々な文字が出現するが，子音なら現れる文字はかなり限定されることから，候補の文字を確定していく
5. 英語の文字の特性(例えばhはeの前によく現れるが，後ろにはめったに現れない)を利用して，文字を確定していく

このように，西暦800年から1200年にかけて，アラビアの学者たちの知的業績は，素晴らしいものであった。数学においても，古代文明の数学の知見はアラビア世界に集約されていた。古代ギ

リシャの数学はもちろん，中国の古代数学もインドやペルシャを通じてアラビアにもたらされていた。アラビア数学は700年にもわたって栄えたが，その頃のヨーロッパにおける数学は暗黒時代であった。いや数学だけではなく，ヨーロッパの科学一般，文化全体が暗黒時代にあったのである。

このようなアラビア数学は，現在でも用いられている用語を残している。

■ゼロ(zero) : アラビア語の「シフル」(何もないという意味)を，ラテン語に音訳した「zephirum」という単語が起源となっている。

■アルゴリズム(algorithm) : 決まった手順，方法という意味であるが，9世紀のアラビアの数学者アル＝フワーリズミーの名前が，ラテン語に訳されるときに勘違いされて伝わったものである。

■アルジェブラ(algebra) : 代数学の意味であるが，アル＝フワーリズミーが著した，『ヒサーブ・アル＝ジャブル・ワル＝ムカーバラ(アルジャブルとアルムカーバラの計算の書)』という本の題名のアル＝ジャブル(方程式の両辺に同じ項を加えるという意味)が，言葉の起源となっている。

さて，換字方式の暗号の解読が頻度分析によってできるようになったので，16世紀のフランスの外交官ヴィジュネルによって，新しい暗号(ヴィジュネル暗号)が考案された。ヴィジュネル暗号は，下のようなヴィジュネル方陣とキーワードで暗号文を作成するのである。

平文	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

［問3］「study mathematics hard」という平文を，「WHITE」をキーワードとしてヴィジュネル暗号化する。暗号化の規則を解明し，暗号文を完成せよ。

キーワード　：　W H I T E W H I T E W H I T E W H I T E

平文　　：　s t u d y m a t h e m a t i c s h a r d

暗号文　　：　O A C

ヴィジュネル暗号以前の暗号は，単アルファベット換字式暗号と呼ばれ，ヴィジュネル暗号は，多アルファベット換字式暗号と呼ばれる。ヴィジュネル暗号は，頻度分析では解読できず，鍵の候補もあまりにも多いので総当りでチェックも出来ない強力な暗号であり，解読不能の暗号と呼ばれていた。しかし，その方法からわかるように，暗号化するのに手間がかかるため，誕生から200年間はほとんど無視されていた。

ときは経て19世紀のイギリスに，科学者チャールズ・バベッジがいた。彼は，現代的なコンピュータのひな形とでもいうべきものを作成するとともに，暗号解読者でもあった。バベッジは，1854年頃にヴィジュネル暗号の解読に成功した。ヴィジュネル暗号は，キーワードによって異なる方法で暗号化されたために出現頻度が平均化され，解読が困難であった。しかし，キーワードの文字数分しか暗号化の方法がないので，よく出てくる単語は暗号文の中にも何度も出現する。そのことを手がかりに，バベッジは解読方法を発見したのだ。ところが，バベッジは解読に成功したことを公表しなかった。一説では，バベッジが解読に成功した時期がクリミア戦争勃発の直後であり，ヴィジュネル暗号の解読はイギリスをロシアに対して優位に立たせるものだったので，イギリス情報部がバベッジに秘密にするように要請したからだという。

この解読の成功により，19世紀末にビジネスマンや軍部は，ヴィジュネル暗号に替わる解読されない暗号を熱望していた。1901年には，イタリアの物理学者マルコーニが無線通信の実験に成功した。無線通信は世界中のどこにでも届くので非常に便利であるが，それは誰にでも傍受できるということでもあった。そのこともあって，第1次世界大戦，第2次世界大戦において，軍部の暗号に対する要求は高まり続けた。

1918年，ドイツの発明家のシェルビウスは，「エニグマ(謎)」と呼ばれる暗号機を発明した。エニグマは，キーボード，プラグボード，3つのスクランブラー，レフレクター，ランプボードからなる暗号作成機である(右図)。

［問4］エニグマの各変数は次の通りである。エニグマの初期設定の数を求めよ。

■3つのスクランブラーは，各々26通りの向きに設定できる

■3つのスクランブラーの順序は交換できる

■プラグボードは，26個の文字から6組のペアを選んでつなぐ

・$26^3 \times 3! \times \frac{{}_{26}P_{12}}{6! \times 2^6} \fallingdotseq 1 \times 10^{16}$　(1京)

この初期設定の数が，エニグマ暗号の鍵となるのである。初期設定(鍵)はコードブックにしるされて，関係者に配布された。エニグマ機が敵の手に渡ったとしても，コードブックがなければ解読は容易ではない。

1926年になって，連合国側の傍受したドイツのメーッセージに，解読できないものが混じり始めた。エニグマの利用が開始されたのである。エニグマの台数が増えるにつれ，イギリス，アメリカ，フランスの情報収集能力は落ち続け，解読を諦めてしまったため，ドイツは世界でいちばん安全な通信手段を持つことになった。しかし，ポーランドの努力とそれを引き継いだイギリス情報部の暗号解読者の奮闘で，エニグマ暗号も解読されることとなった。

その最大の立役者は，1911年生まれのイギリスの天才数学者，アラン・チューリングである。チューリングを中心とする暗号解読チームは，数学者を中心に構成されていた。昔の暗号解読の中心は言語学者であったが，この時代には数学者が活躍していたのである。

チューリングは，1930年代に仮想的な機械「チューリングマシン」を考えだし，その内部の仕組みを変更することにより，どんなタイプの機械にもなれる「万能チューリングマシン」を構想したことで有名であり，計算機科学，人工知能の父と呼ばれている。

このチューリングが考えだしたチューリング・テストは，「機械は思考できるか？」という問題意識から提案されたテストである。コンピューターと人間が，お互いに見えないように壁を隔てて，キーボードとディスプレイで対話する。この対話のみでは壁の向こうの相手がコンピューターか人間か判定できないなら，それは人間と変わらない，つまりコンピュータは意識をもっていると考えていい，とチューリングは考えたのである。

2014年6月7日にイギリスのレディング大学で行われた英国王立協会のイベントで，「ユージーン・グーツマン」は審査員の33%に「人間」と判定された。このユージーンは少年ではなく，ロシアのサンクト･ペテルブルクのチームが設計したスーパーコンピュータである。ユージーンは，5分間にわたるキーボードを使った一連の会話で，本物の人間である全審査員の33%を欺くことに成功した。これによってユージーンは，チューリング・テストに公式に合格した最初の人工知能になった。

［問5］人工知能，2045年問題，映画『トランセンデンス』は知っている？

2. コンピュータによる暗号作成と解読

エニグマ暗号の解読機「ボンブ」を作ったチューリングは，1954年に自殺してその生涯を閉じた。彼は暗号解読で祖国イギリスを守ったのであるが，その功績は一般には知られることはなかった。このように，機密を守るために暗号解読者たちの働きは公にされることはなかったが，その後も新たに開発されたローレンツ暗号に対しても解読機が作成され，というように，暗号の作成者と解読者の戦いは続いた。

第2次世界大戦後コンピュータが発明され，その性能の向上と価格の低下もあって1960年代には，国家だけではなく企業も含めてコンピュータによる暗号の作成と解読の時代となった。暗号作成者は鍵を1つ決め，コンピュータで暗号を作成する。その暗号文を受け取った利用者は，作成に利用された鍵を使って暗号を解読するのである。

［問6］コンピュータによって非常に強力な暗号が簡単に作成でき，その解読もすぐにできる時代となったが，暗号利用者全員が頭を悩ませている問題が1つあった。それは何か？

・鍵の受け渡しを安全に行う方法がない！

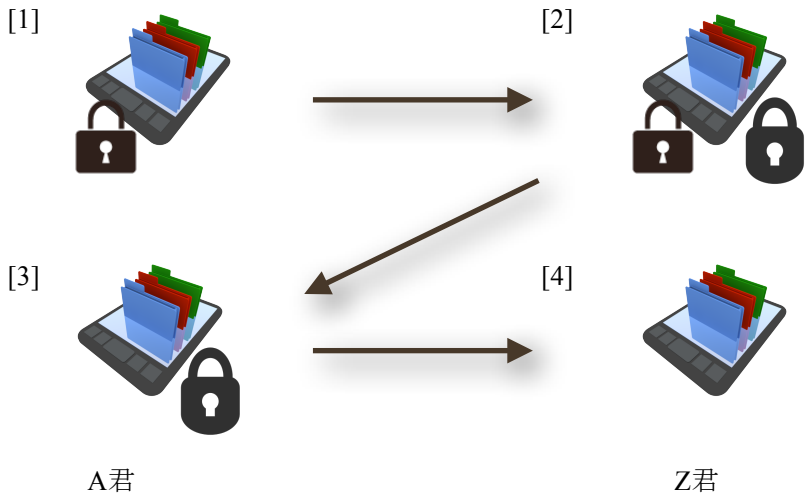
上記の問題について，次のような方法で解決できると考えた人がいた。

[1]　A君は，箱に書類を入れて南京錠をかけ，Z君に送る。

[2]　Z君は，箱にさらに自分の南京錠をかけ，A君に送り返す。

[3]　A君は，自分の南京錠を外し，Z君に送り返す。

[4]　Z君は，自分の南京錠を外して，箱から書類を取り出して読む！



［問7］2重南京錠で，先の鍵の配送問題は解決できたように思える。[1]〜[4]の方法を，暗号作成・解読の言葉で言い直してみよ。そして，問題が解決できたかどうかを確認せよ。

[1]　A君は，　　，Z君に送る。

[2]　Z君は，　　，A君に送り返す。

[3]　A君は，　　，Z君に送り返す。

[4]　Z君は，　　，読む！？

(あなたの意見)

(確認)

A君の鍵

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
R	C	H	X	A	G	W	B	S	O	L	D	E	K	Q	F	N	M	Z	I	S	U	Y	J	V	P

Z君の鍵

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
H	I	Q	R	P	A	Y	B	C	L	U	Z	K	S	J	F	T	E	N	G	W	D	X	M	V	O

・平文　　I am very happy

・A君の鍵によるエンコード　　S RE UAMV BRFFV

・Z君の鍵によるエンコード

・A君の鍵によるデコード

・Z君の鍵によるデコード

(結論)

箱に2重のカギをかける考え方は，暗号には使えなかったが，鍵の配送の問題を解決する1つのきっかけとなった。つまり，暗号システムの研究者たちにとって，次のことが方向として見えてきたのである。

■南京錠が2重であることは，はずす鍵が違うので安全であった。

■しかし，はずす順序が問題となるので，南京錠は1つであることが望ましい。

■つまり，南京錠とそれを開ける鍵を考え，鍵を何らかの方法で安全に共有すべき。

■従来の暗号システムは，同じ鍵を使ってエンコード，デコードを行ってきた (対称的)。

■そこで，エンコードの鍵とデコードの鍵を違うものにできないものか(非対称的)？

3. 公開鍵暗号方式

コンピュータによる暗号化は，ある数(平文)を他の数(暗号文)に変換することであり，これは数学的に言えば関数である。エンコード(暗号化)とデコード(復号化)の鍵が同じであることは，関数で言えば，例えば次のようになる。

(例)　f(x)＝2x

が鍵であるとすると，f(x)の逆関数は，

$$f^{-1}(x)=\frac{1}{2}x$$

である。そして，

f(12)＝24

と12がエンコードされると，

$f^{-1}(24)=12$

と24が簡単にデコードできる。

暗号研究者たちが探し求めたのは，逆関数が簡単に見つからない関数なのだ。このような関数を用いて，エンコードの鍵とデコードの鍵が同じでない，非対称鍵暗号を作ろうというのである。そして行き着いたのが，天才数学者ガウスが「数学の女王」と呼んだ整数論の素数と合同式であった。

この公開鍵暗号方式の概要は，次の通りである。

[1]　南京錠が暗号化の鍵，それを開ける鍵が復号化の鍵である。

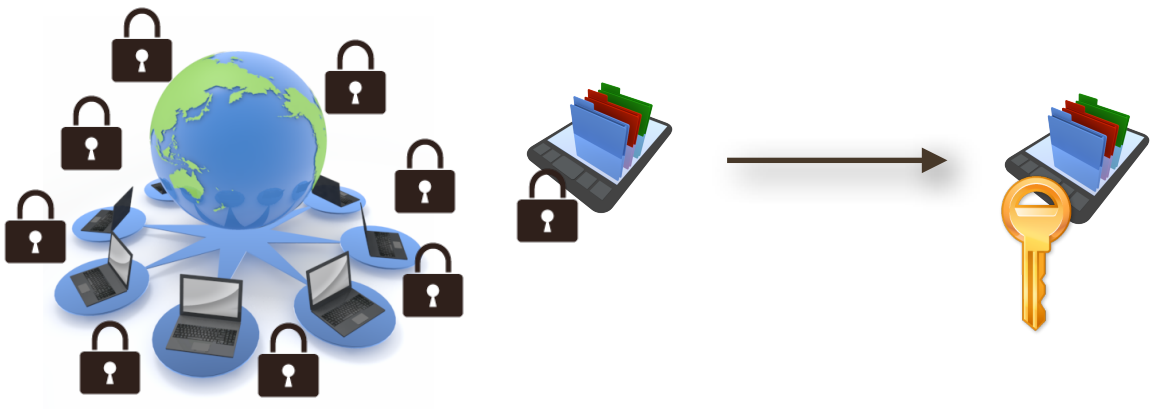
[2]　A君は南京錠とそれを開ける鍵を設計(作成)する。

[3]　A君はインターネット上に南京錠を配布し，解錠する鍵は秘密にする。

[4]　A君にものを送りたい人は，公開されている南京錠をかけて暗号化する。

[5]　A君以外の人には鍵がないので，送られたものを途中で見られても安全である。

[6]　A君は届いた南京錠のかかったものを，鍵で開ける(復号化する)ことができる。



4. RSA暗号

現代社会を支えるテクノロジーのひとつである公開鍵暗号方式である，1977年に発明されたRSA暗号(Ron Rivest・Adi Shamir・Len Adlemanの頭文字)の基盤となっているのは，素数と合同式である。素数と合同式の学習を通じて，RSA暗号の仕組みの概要を理解しよう。

［問8］次の整数を素因数分解せよ。

(1)　12　　(2)　135

(3)　34650　　(4)　108953

［定義］

a，b，pは整数で，p≧2とする。a−bがpの倍数であることを

$a \equiv b \pmod{p}$　・・・(*)

と表す。

すなわち，kを整数とするとき，

$a \equiv b \pmod{p} \Leftrightarrow a-b=kp \Leftrightarrow a=kp+b$

特に，0≦b＜pのとき，

$a \equiv b \pmod{p}$ ⇔ aをpで割ったときの余りがb

[補足]

(1)　(*)の式を合同式という。

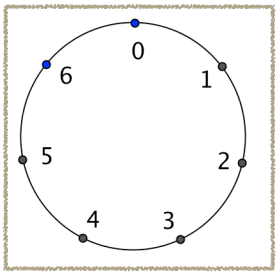
(2)　(*)は「a合同bモッドp」と読む。また，「aとbはpを法として合同である」とも言う。

［問9］次の合同式の計算を行え。

(1)　$12\equiv$　$(\mathrm{mod}\ 10)$　　(2)　$40\equiv$　$(\mathrm{mod}\ 7)$

(3)　$123456\equiv$　$(\mathrm{mod}\ 2)$　　(4)　$112\equiv$　$(\mathrm{mod}\ 6)$

合同式を考えることは，時計の文字盤上での計算に例えられる。右図は，mod7の計算のときの時計盤である。また，合同式の計算を，モジュラー算術ということもある。



モジュラー算術では，次のように簡単な関数も逆対応がわからなくなる。

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x \pmod 7$	3	2	6	4	5	1

[定理1]

以下，文字はすべて整数とし，mod pを省略する(p≧2)。

1．a≡bのとき

(1)　a＋c≡b＋c　　(2)　a−c≡b−c　　(3)　ac≡bc　　(4)　$a^c \equiv b^c$

2．a≡b，x≡yのとき

(1)　a＋x≡b＋y　　(2)　a−x≡b−y　　(3)　ax≡by

［問10］定理1を証明せよ。

［問11］下の表を利用して，21を法とする世界における次のべき乗を求めよ。

(1)　5^4＝　　(mod 21)　　(2)　11^6＝　　(mod 21)

(3)　17^7＝　　(mod 21)　　(4)　20^{13}＝　　(mod 21)

21を法とする世界の数	べき乗数																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	11	1	2	4	8	16	11	1	2	4	8	16	11
3	3	9	6	18	12	15	3	9	6	18	12	15	3	9	6	18	12
4	4	16	1	4	16	1	4	16	1	4	16	1	4	16	1	4	16
5	5	4	20	16	17	1	5	4	20	16	17	1	5	4	20	16	17
6	6	15	6	15	6	15	6	15	6	15	6	15	6	15	6	15	6
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
8	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8
9	9	18	15	9	18	15	9	18	15	9	18	15	9	18	15	9	18
10	10	16	13	4	19	1	10	16	13	4	19	1	10	16	13	4	19
11	11	16	8	4	2	1	11	16	8	4	2	1	11	16	8	4	2
12	12	18	6	9	3	15	12	18	6	9	3	15	12	18	6	9	3
13	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13
14	14	7	14	7	14	7	14	7	14	7	14	7	14	7	14	7	14
15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
16	16	4	1	16	4	1	16	4	1	16	4	1	16	4	1	16	4
17	17	16	20	4	5	1	17	16	20	4	5	1	17	16	20	4	5
18	18	9	15	18	9	15	18	9	15	18	9	15	18	9	15	18	9
19	19	4	13	16	10	1	19	4	13	16	10	1	19	4	13	16	10
20	20	1	20	1	20	1	20	1	20	1	20	1	20	1	20	1	20

［問12］上の21を法とする世界のべき乗の表を見て，mod21における数aと，べき乗数bとの美しい関係を発見せよ。

・$a^7 \equiv a \pmod{21}$，$a^{13} \equiv a \pmod{21}$

問12で発見した美しい関係は，実は一般的に成り立つのである。

［定理2］

任意の2つの異なる素数p，qの積pqを法とする世界では，p−1とq−1の最小公倍数をL，任意の自然数をnとすると，整数aに対して次のことが成立する。

$a^{nL+1}=a \pmod{pq}$,　　$a^{n(p-1)(q-1)+1}=a \pmod{pq}$

［問13］21を法とする世界について，定理2が成立することを確認せよ。

RSA暗号は，次の要領で暗号化する方法である。

[1]　適当な2つの素数p，qの積pqを法とする世界で考える

[2]　平文を数値化したaを(a＜pq)，適当な数Eでa^Eとして暗号文の数値に変換する

[3]　このとき，「法はpq，鍵はE」であることは公開する(公開鍵方式)

［問14］RSA暗号を作成する。21を法とし，公開鍵E＝5として，次の平文を暗号文に変換せよ。

「2　　5　　11　　16　　19」

［定理3］

2つの異なる素数p，qの積pqを法とし，公開鍵Eで平文AをRSA暗号法で暗号化したとき，復号する鍵Dは，

$(A^E)^D=A^{n(p-1)(q-1)+1} \pmod{pq}$

を満たす数であるから，

$$D=\frac{n(p-1)(q-1)+1}{E}$$

［問15］問14で作成した暗号文が，定理3から得られる鍵Dで復号できることを確認せよ。

［問16］2つの異なる素数p，qから作った積pqと鍵Eを公開すると，復号するための鍵Dが定理3から簡単に得られるために，RSA暗号は簡単に復号できるように思える。ところが，RSA暗号は軍事，外交，通商，犯罪など，あらゆる場面で利用されている。つまり，RSA暗号を破るのは，極めて困難(実質的に不可能)とされているのである。その理由は何であるかを考えよ。

・積pq(計算結果)は簡単に求められて公開されているが，その積は非常に大きな数なので，因数分解は極めて困難である

［問17］Wolfram Alphaを利用して，次の実験を行なえ。そして，命令の意味を理解し，自分で他の実験も行うことで，問16で考えたことを確認せよ。

■Prime(1000000)

■Prime(1000000)*Prime(10000001)

■FactorInteger(2778546183643333)

5. RSA暗号の解読困難さ

RSA暗号の素晴らしいところは，鍵の交換に関する問題を一挙に解決したことである。南京錠にあたるエンコードするための公開鍵(素数の積pqとE)は全世界に公開し，デコードするための個人の鍵(素数pとq)を秘密にしておけばよいのである。

このように，RSA暗号は素因数分解の困難さを基盤としている。素因数分解については，次のような事実がある。

■RSA暗号が世間に紹介されたのは，1977年8月の『サイエンティフィック・アメリカン』誌のコラム「数学ゲーム」に，マーティン・ガードナーが問題を出したときのことである。そのコラムでガードナーは，次の数の素因数分解ができるか？　と読者に挑戦した。

N=114381625757888867669235779976146612010218296721242362562561842935706935245733897
830597123563958705058989075147599290026879543541

これは129桁の数であり，素因数分解が完成したのは17年後の1994年4月であった。600人のボランティアが参加したチームが，世界各地のコンピュータをネットワークで結び，ついに次の2つの素数p，qの積であることを解明した。

p=3490529510847650949147849619903898133417764638493387843990820577

q=3276913299326670954996198819083446141317764296799294253979828853 3

■2010年1月11日の新聞記事から

・NTTが232桁の整数(2進数で768ビット)の素因数分解に成功した(世界記録，従来は200桁)

・この素因数分解は，300台のパソコンによる並列計算で約3年かけて解いたものである

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

=33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

×36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917

■実用化されたRSA暗号では，最低でも77桁程度の2つの素数p，qを用意し，それを掛け合わせた155桁程のpqを法としてきた

■現在のRSA暗号では，一般的には素数と素数を掛け合わせた後の法とする数が，310桁にもなる数を用いている

■p，qに利用する素数は，いま実際に使われている155桁程度以下のものなら，10^{150}個以上は存在することが分かっているが，これは宇宙の原子の数(10^{80}〜10^{100})以上である

■これらから得た公開鍵・秘密鍵は，世界中の人々はもとより，あらゆる生命に1つずつ割り当てたとしても，使い果たすことはない

6. 量子コンピュータ・量子暗号

これまで見てきたように，RSA暗号の安全性は完璧な安全性ではなく，素因数分解に天文学的な時間がかかることに基づく安全性であった。つまり，コンピュータの性能が格段に向上し，実用的な時間で素因数分解ができれば，RSA暗号は解読されるのである。

アメリカ国家安全保障局NSA(National Security Agency)が，どのような暗号でもほぼ解読が可能な「量子コンピュータ」の開発に取り組んでいると，2014年1月にワシントン・ポストが報じた。NSAの元契約職員エドワード・スノーデンが暴露した文書に基づく情報だという。NSAは，世界中でいちばん多くの数学者を雇用している機関だと言われている。

量子コンピュータは，量子力学の理論に基づいたコンピュータであり，従来のコンピュータとは全く違う考え方で作られていて，分野によっては物凄いスピードで計算ができる。そして，20年ほど前にアメリカのベル研究所が，「量子コンピュータが完成すれば，いままでとは比較にならない短時間で計算が行えるので，公開鍵暗号(RSA暗号，楕円曲線暗号)はすべて解読される」ということを数学的に証明した。情報処理の仕組みが全く異なり、大量の素因数分解を一挙に計算できる量子コンピュータは，この種の暗号を解くことは大得意なのである。量子コンピュータを使えば，国家の最高機密も解読されてしまうので，専門家たちの間で大騒ぎになった。

そこで，1984年にIBMの研究によって提案されたが，有効性が不明であり，通信手段もなかったせいで忘れられていた「量子暗号」が脚光を浴びることとなった。1997年に，

　　量子暗号は量子コンピュータでも破れない

ことが証明されたので，量子暗号技術の実用化に向けて，研究が加速することになった。

現行の暗号は，

　　情報を盗むことはできても解読に時間と手間がかかるために，秘密は保持できる

という安全性であった。それに対して量子暗号は，

　　盗聴(情報を盗むこと)そのものができない仕組み

なのである。盗聴したとしても，盗聴の事実が発信者，受信者の両方に知られてしまう暗号なのだ。それは，量子暗号が

　　光は波であり，同時に粒子(光子という)である

という光の量子的性質を利用しているからである。

［問17］§4の内容で，よくわからなかった事項，興味をもった事項について調べ，レポートを提出せよ。

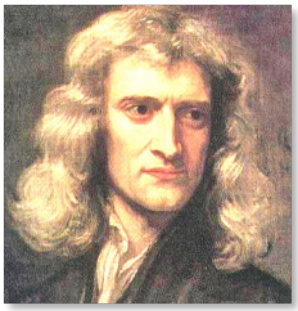
第 3 章　数学と自然　－ 君は $E=mc^2$ を観たか －

§1　2 人の天才ニュートンとマクスウェル

19 世紀末から 20 世紀の初頭にかけて，物理学者は 2 つの偉大な科学の体系の間に存在する矛盾に悩んでいた。その 2 つの科学体系とは，

ニュートン力学とマクスウェルの電磁気学

であった。



ニュートン力学は，イングランドの天才数学者・物理学者ニュートン(1642～1727)が創始した力学であり，その時代まで 200 年にわたって使われ続け，あらゆる事柄を完璧に説明していた。ニュートン力学は，絶対時間と絶対空間を前提としていて，特別優遇された時間も空間も存在しないとし，「運動の相対性原理」

物理法則は運動の方向，運動の速さ，遅さには関係なく，
一定の速度で運動しているものには同じである

を含んでいた。例えば，走る電車の中でジャンプをしても，動いていないときと同じ地点に着地できる。また，100km/h で飛ぶ鳥を地上からみれば 100km/h に，60km/h で同じ方向に走る車から見れば 40km/h に，同じ方向に 100km/h で走る車から見れば止まって見える。このように，相対性原理はニュートン力学の中心にあった。

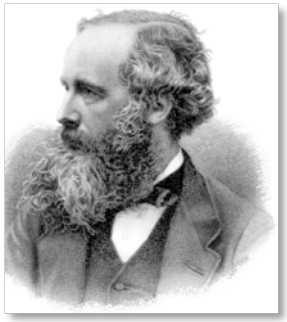
一方で，スコットランドの物理学者マクスウェル(1831～1879)が考えだした新しい概念の電磁場は，次の 4 つのマクスウェルの方程式で完璧に記述されていた。

$$\nabla\cdot\mathbf{E}=4\pi\rho$$ ← 電場がどのように生み出されるかを表す

$$\nabla\times\mathbf{B}-\frac{1}{c}\frac{\partial\mathbf{E}}{\partial t}=\frac{4\pi}{c}\mathbf{J}$$ ← 電流と変化する電場がどのように磁場を生じるかを表す

$$\nabla\times\mathbf{E}+\frac{1}{c}\frac{\partial\mathbf{B}}{\partial t}=0$$ ← 変化する磁場がどのように電場を生み出すかを表す

$$\nabla\cdot\mathbf{B}=0$$ ← 磁気単極子は存在しないことを表す



これらの方程式から生まれた電磁気現象に関する研究から，ラジオ，テレビ，電子レンジ，レーダー，無線通信，電子機器などが誕生したのである。

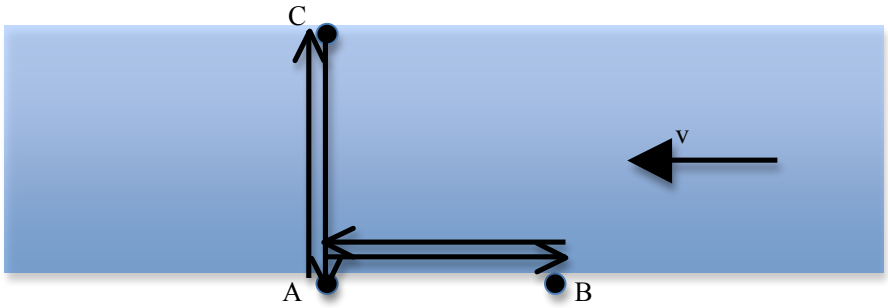
このマクスウェルの電磁気理論の中心には，「光速一定の原理」があった。音の速度は，音源の速度に関わらず一定である(例えば，15℃では 340m/s)。これは，音波を伝える空気などの媒体の性質による。マクスウェルの方程式によれば，光もまた光源の速度に関わらず一定の速度 30 万 km/s で伝わる。当時の物理学者たちは，これは光がエーテルという媒体の中を運動しているからだと考え，エーテルの性質が光の速度を決定していると推測した。

もし光の速度が一定なら，絶対時間と絶対空間，相対性原理のニュートン力学の中に，特別な存在の座標系(慣性系)が存在することになる。さて，ニュートンとマクスウェルの理論の，どちらが正しいのだろう。それを確かめるべくある実験が行われ，その結果を基に新たな考えが生まれてきた。

§2　マイケルソンとモーリーの実験

まず，次のような例を考える。

幅が s，流れの速さが v の川がある。その川岸の地点 A から上流に s だけ進んだ地点を B，A の岸に垂直な対岸の地点を C とする(下図)。

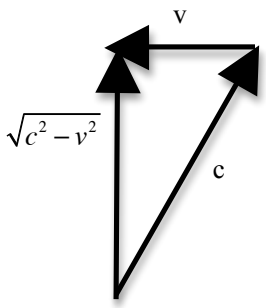


この川を速さ c で泳ぐ人が，A から B まで往復する時間を t，A から C まで往復する時間を t’として，これらの時間を求める。

A→B→A と往復する時間は，

$$t=\frac{s}{c-v}+\frac{s}{c+v}=\frac{2cs}{c^2-v^2}\cdots(2\text{−}1)$$

A→C→A と往復する時間を考える。A から C に到着するためには，右図のように A から上流側に泳がなくてはならず，そのときの速度は，



$$\sqrt{c^2-v^2}$$

である。C から A に戻るときも同様なので，往復する時間は，

$$t'=\frac{s}{\sqrt{c^2-v^2}}+\frac{s}{\sqrt{c^2-v^2}}=\frac{2s\sqrt{c^2-v^2}}{c^2-v^2}\cdots(2\text{−}2)$$

ここで，$c>\sqrt{c^2-v^2}$ であるから，(2−1)，(2−2)より，

$$t>t'$$

となる。つまり，

同じ距離を往復する場合，流れに沿って往復する方が垂直方向より時間がかかる

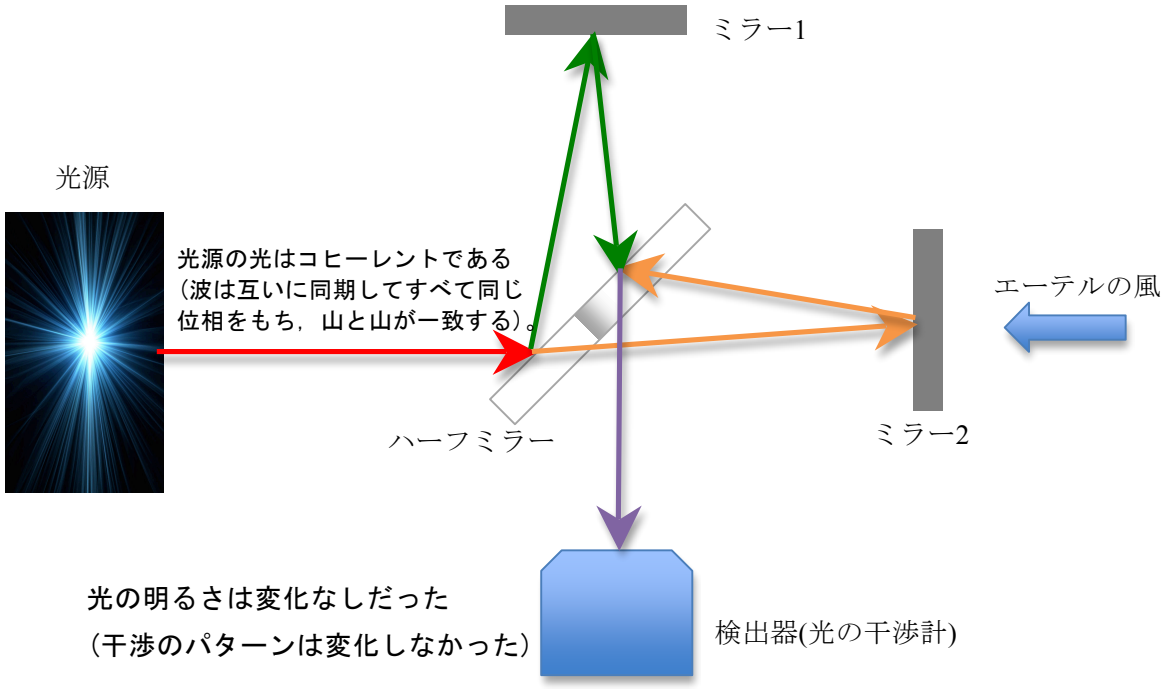
ことが分かる。

上の例と同じく，エーテルはその中を伝わる光を動かすので，光がエーテルの運動方向に沿って伝わるときと，運動方向に垂直に伝わるときとでは速度が違ってくるはずだ，と当時の物理学者たちは考えた。この考えを，1881 年と 1887 年に精密な実験装置で実際に実験したのが，アメリカの 2 人の物理学者マイケルソン(1852～1931)とモーリー(1838～1923)であった。地球の自転方向と，それに対して垂直な方向の 2 つの光の速度を測定し，光速の違いを見つけようとしたのである。次ページの図で，コヒーレントな光がハーフミラーで別れてから，ミラー1，2 で反射して再びハーフミラーまで戻ってくる距離は同じである。もし，光速に違いが出るなら，計算で 0.2 波長のずれ(位相差)が生じて干渉が起こり，光は暗くなるはずであったが，実験結果の位相差は 0.2 波長よりもずっと小さいものであった。つまり，

エーテルの風の影響は検出できず，光速はどちらの方向も 30 万 km/s で一定である

というものであった！

■マイケルソン・モーリーの実験



運動の方向にかかわらず光速は一定であるという実験結果に，物理学者たちは困惑した。ニュートン力学かマクスウェルの電磁気学のどちらかに何か間違いがあるということになったからだ。

§3　ローレンツ変換

オランダの物理学者ローレンツ(1853～1928)は，マイケルソン・モーリーの実験結果を説明し，ニュートン力学とマクスウェルの電磁気学を合致させるために，次のように考えた。

宇宙空間には，光の媒体となるエーテルという仮想物質が満ちている。エーテルに逆らって進む物体は，エーテルの圧力を受けて縮む。また，光速は常に一定であり，運動している観測者にも，静止している観測者にも同じ速度で見えるためには，運動している観測者の時間は遅くなる。

そしてローレンツは，エーテルの中を進む光の速度は一定であるとして，静止している慣性系と運動している慣性系の間の長さと時間の違いを説明できる，次のような変換式を作り上げた。

■ローレンツ変換

XY 平面が静止しているエーテルに対して固定され，別の X'Y'平面が地球に張り付いて速度 v で地球とともに動いている。X'は X に沿って，Y'は Y と平行に動くとき，座標と時間の組について，次の変換式が成り立つ。

$$x'=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}(x-vt),\quad y'=y,\quad z'=z,\quad t'=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}\left(t-\frac{v}{c^2}x\right)$$

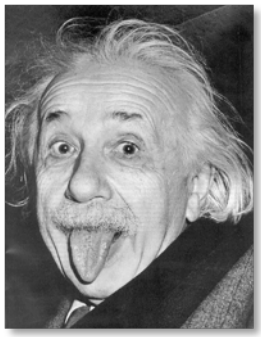
ローレンツ変換は，確かに実験結果を正しく表していたが，物理的な意味はなく，単なる経験式でしかなかった。この式に，物理的な意味を与えたのが，天才アインシュタインであった。

§4　天才アインシュタイン登場

ドイツの天才物理学者アインシュタイン(1879～1955)は，16 歳の頃に次のような子どもらしい思考実験を行った。

光速で移動している自分が，自分と平行に移動している光線の方を見ると，どんなことが起こるだろう？

［問 1］アインシュタインと同じ思考実験を行い，考えをまとめよ。



この一見，単純な質問に対する答えは，当時の物理学では得られなかった。そこでアインシュタインは，思索を積み重ねて次の考えに達したのである。

・エーテルという仮想物質を考える必要はなく，エーテルは存在しない
・光速 c はどこで測っても不変である
・光速 c を不変に保つように，時間の流れが変わるのである

つまり，アインシュタインは，エーテルの存在も否定し，

光速度不変の原理 ：光速 c は観測者の速度によらずに一定である 相対性原理　　：等速度で動くものの中では，物理法則は全く同じである

という 2 つの原理のみから出発して，次の「特殊相対性理論」を創りあげた。

1. 速く動く物体ほど，その時間はゆっくり進んで見える
2. 物体の長さは，動く方向に向かって縮んで見える
3. 物体は速く動くほど，質量が増えて見える
4. 静止した物体は，エネルギー$E=mc^2$をもつ(c：光速度，m：物体の質量)

アインシュタインは，高速度では空間と時間は収縮し，絶対空間・絶対時間は存在せず，光速度が速度の上限であることを示したのである。これから，順を追ってこのことを学んでいこう。その際，数学が非常に重要な武器となる。しかも，最後の方を除いて，利用する数学は中学数学程度ですむのである。数学が，自然科学の言語として強力であることの一例となっている。

§5　時間が遅れる

アインシュタインは，次のような思考実験を行った。

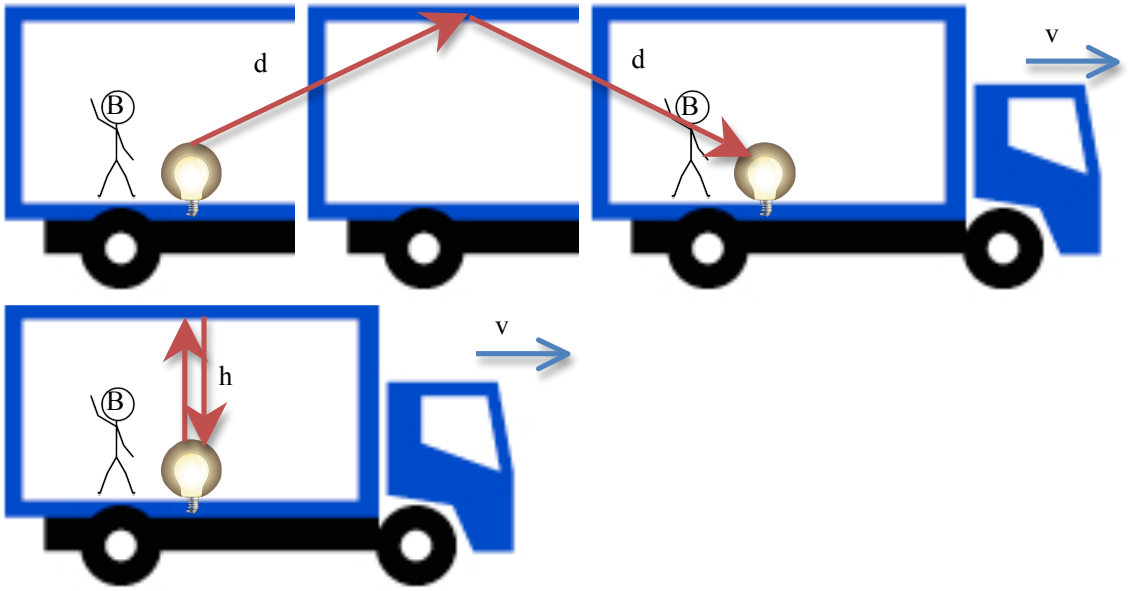
高さ h のトラックの荷台に積まれた光源から光が発せられて，天井で反射して光源に戻る様子を観察する。トラックの外の地面には A がいて，トラックの荷台には B が乗っている。トラックは A の前を速度 v で通過した。このとき，A が t 秒間で見た光の経路と，B が t’秒間で見た光の経路はそれぞれ次のページの図のようになる。

ここで，光速 c が一定であるとすると，

$2d=ct$，$2h=ct'$

$d>h$ であるから，$ct>ct'$

よって，$t>t'$



すなわち，静止している A から見た方が時間が長くかかる。言い換えると，静止している A にとっては動いている B よりも時間が速く過ぎ，動いている B にとっては静止している A よりも時間が遅く過ぎることになる。

そこで，時間の遅れを実際に計算する。まず，A に関しては，

$$\mathrm{d}=\sqrt{h^2+\left(\frac{1}{2}vt\right)^2}$$

より，

$$\mathrm{c}=\frac{2d}{t}=\frac{2\sqrt{h^2+\left(\frac{1}{2}vt\right)^2}}{t}\cdots(4\text{−}1)$$

次に，B に関しては，

$$\mathrm{c}=\frac{2h}{t'}\cdots(4\text{−}2)$$

(4−1)，(4−2)より，

$$\frac{2\sqrt{h^2+\left(\frac{1}{2}vt\right)^2}}{t}=\frac{2h}{t'}$$

2 乗すると，

$$\frac{4\left(h^2+\frac{1}{4}v^2t^2\right)}{t^2}=\frac{4h^2}{t'^2}$$

(4−2)より，2h＝ct'であるから，

$$\frac{c^2t'^2+v^2t^2}{t^2}=\frac{c^2t'^2}{t'^2}$$

よって，

$$\mathrm{c}^2\left(\frac{t'}{t}\right)^2=\mathrm{c}^2-\mathrm{v}^2$$

$$\left(\frac{t'}{t}\right)^2 = 1-\left(\frac{v}{c}\right)^2$$

t＞0，t'＞0，c＞v であるから，

$$\frac{t'}{t} = \sqrt{1-\frac{v^2}{c^2}}$$

よって，

$$t = \frac{1}{\sqrt{1-\frac{v^2}{c^2}}}t' \cdots (4-3)$$

通常は，トラックの速度は光速 c と比べて非常に小さい(v<<c)ので，この場合は，

$$\frac{v^2}{c^2}=0 \quad より，\quad \sqrt{1-\frac{v^2}{c^2}}=1$$

と見てよく，このとき(4−3)は t＝t'となり，日常感覚と同じである。

ところが，トラックの速度 v が光速の 98％だったとすると，(4−3)において，

$$v=0.98c$$

より，

$$\sqrt{1-\frac{v^2}{c^2}} = \sqrt{1-\frac{(0.98c)^2}{c^2}} = \sqrt{1-0.9604} \fallingdotseq \sqrt{0.04} = 0.2$$

よって，

$$t = \frac{1}{0.2}t' = 5t'$$

つまり，0.98c で運動する B が 1 秒過ぎるたびに，A は 5 秒過ぎることになる！

§6　ローレンツ変換を導く

アインシュタインが設定した 2 つの原理である光速度不変の原理，相対性原理から，ローレンツ変換を導く。ローレンツは，マイケルソン・モーリーの実験結果を説明するために経験式としてローレンツ変換を導いたが，アインシュタインはそれに物理的な意味を与えたのである。

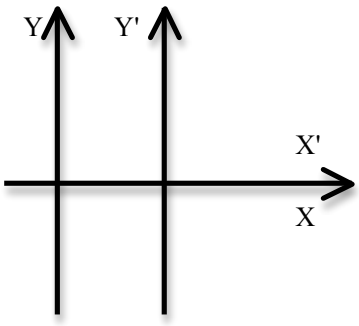
以下，2 つの慣性系(一定速度で動く観測者)K，K'があり，X'軸は X 軸に沿って，Y'軸は Y 軸と平行に相対速度 v で動いているとする(空間は x 座標の変化だけを考える)。

光が発せられた瞬間，K と K'は同じ場所にいたとすると，光速度は一定なので，その後の t 秒後の K，t'秒後の K'の位置はそれぞれ，

$$x=ct \quad \Leftrightarrow \quad x-ct=0 \quad \cdots(6-1)$$

$$x'=ct' \quad \Leftrightarrow \quad x-ct'=0 \quad \cdots(6-2)$$

と表される。



［問 2］(6−1)，(6−2)を用いて，

ガリレイ変換：t'＝t，x'＝x−vt

を，光速度不変を満たすように改変したい。このとき，x'，t'への変換式を，x，t の 1 次式としてよい理由は何か。

・$x'=x^n$ (n≧2)なら，$x=x'^{\frac{1}{n}}$ となり，相対性原理を満たさないので，1 次式でなければならない。

(6−1)，(6−2)より，λを定数として，

$x'-ct'=\lambda(x-ct)$　・・・(6−3)

とおくことができ，同時に反対方向を考えると，μを定数として，

$x'+ct'=\mu(x+ct)$　・・・(6−4)

とおくことができる。

(6−3)＋(6−4)より，

$$x'=\frac{\lambda+\mu}{2}x-\frac{\lambda-\mu}{2}ct$$

(6−4)−(6−3)より，

$$ct'=\frac{\lambda+\mu}{2}ct-\frac{\lambda-\mu}{2}x$$

となるので，

$$\frac{\lambda+\mu}{2}=a,\quad \frac{\lambda-\mu}{2}=b$$

とおくと，

$x'=ax-bct$　・・・(6−5)

$ct'=act-bx$　・・・(6−6)

(6−5)より，x'＝0 であれば，

$$x=\frac{bct}{a}\cdots(6-7)$$

x'＝0 のとき，K については，

$x=vt$

であるから，(6−7)より，

$$vt=\frac{bct}{a}\quad\Leftrightarrow\quad v=\frac{bc}{a}\cdots(6-8)$$

次に，K の視点からは，t＝0 のとき，(6−5)より，

$$x'=ax\quad\Leftrightarrow\quad x=\frac{x'}{a}\quad\cdots(6-9)$$

K'の視点からは，t'＝0 のとき，(6−6)より，

$bx=act$　・・・(6−10)

(6−5)より，

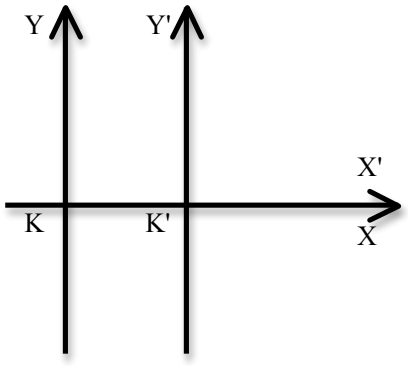
$$t=\frac{ax-x'}{bc}$$

ゆえに，(6−10)に代入して，

$$bx=\frac{ac(ax-x')}{bc}\quad\Leftrightarrow\quad b^2x=a^2x-ax'$$

よって，

$$x'=a\left(1-\frac{b^2}{a^2}\right)x\quad\cdots(6-11)$$



(6−8)より，$\frac{b}{a}=\frac{v}{c}$であるから，(6−11)は，

$$x'=a\left(1-\frac{v^2}{c^2}\right)x \quad \cdots(6-12)$$

となる。

(6−9)は，K の立場からは，

K'が「真の」値 x を求めるには x'に$\frac{1}{a}$をかけなければならない

と K'に言うことを示し，逆に(6−12)は，K'の立場からは，

K が「真の」値 x'を求めるには x に$a\left(1-\frac{v^2}{c^2}\right)$をかけなければならない

と K に言うことを示している。

このように，2 人の観測者 K，K'はそれぞれ自分の測定値が「真の」値だと考えて，相手に補正をするように言う。このときの補正の式は違っているが，その違いは 2 人が相対運動をしている結果として出てくるものなので，補正の絶対値は等しい。ゆえに，(6−9)，(6−12)より，

$$\frac{1}{a}=a\left(1-\frac{v^2}{c^2}\right) \quad \Leftrightarrow \quad a^2=\frac{1}{1-\frac{v^2}{c^2}}$$

よって，$a=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$

これと，(6−8)からの bc＝av を(6−5)に代入して，

$$x'=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}(x-vt)\cdots(6-13) \quad \left(1>\frac{v^2}{c^2}\text{ より，}v<c\text{，すなわち，光速を超えない。}\right)$$

次に，(6−13)と x＝ct，x'＝ct'より，

$$ct'=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}(ct-vt)$$

よって，$t'=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}\left(t-\frac{vt}{c}\right)$

ここで，$t=\frac{x}{c}$より，

$$t'=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}\left(t-\frac{v}{c^2}x\right)\cdots(6-14)$$

これで，光速度不変の原理，相対性原理からローレンツ変換が導かれた。

式を簡単にするために，

$$\beta=\frac{v}{c},\quad \gamma=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}=\frac{1}{\sqrt{1-\beta^2}}$$

とおくと，ローレンツ変換は次のように表される。

$$x' = \gamma (x - c\beta t) \quad \cdots(L1), \quad t' = \gamma \left(t - \frac{\beta}{c} x\right) \quad \cdots(L2)$$

ローレンツ変換(L1)，(L2)を，(x'，t')から(x，t)に変換する式に書き換える。K から見て K'が速度 v で動くことは，K'から見て K が−v で動くことになるので，(L1)，(L2)において，v を−v に置き換えればよい。

すなわち，次のようになる。

$$x = \gamma (x' + c\beta t') \quad \cdots(R1), \quad t = \gamma \left(t' + \frac{\beta}{c} x'\right) \quad \cdots(R2)$$

［問 3］(L1)，(L2)を実際に x，t について解くことで，(R1)，(R2)が正しいことを確認せよ。

§7　空間と時間が収縮する

ローレンツ変換により，2 つの慣性系(一定速度で動く観測者)の空間と時間の変換が行われることがわかった。ニュートン力学で考えられていた絶対空間・絶対時間は存在せず，慣性系ごとに測定値や時間は違ってくるのである。ここでは，どれだけの違いが現れるのかを考える。

1. 棒の長さについて

地上で観測する人を A，速度 v で飛ぶ飛行機の中の人を B とし，長さ l_0 の棒を 2 本用意して 1 本ずつ地上と飛行機の中において測定する。

■飛行機の中の棒を，地上の A が観測する

B の棒の左端の座標を x_1'，右端の座標を x_2'とすると，B が飛行機の中で測った棒の長さは，

$$l_0 = x_2' - x_1'$$

である。

次に，地上の A が飛行機の中の棒を観測する。棒の左端が座標 x_1 に来たときの時刻を t_1，その同時刻($t_2 = t_1$)に棒の右端の座標を観測すると x_2 であったとすると，A が観測する棒の長さは，

$$l = x_2 - x_1$$

である。

ここで，(L1)より，

$$x_1' = \gamma (x_1 - c\beta t_1) \cdots ①$$

$$x_2' = \gamma (x_2 - c\beta t_2) \cdots ②$$

②−①より，

$$x_2' - x_1' = \gamma \{(x_2 - x_1) - c\beta (t_2 - t_1)\}$$

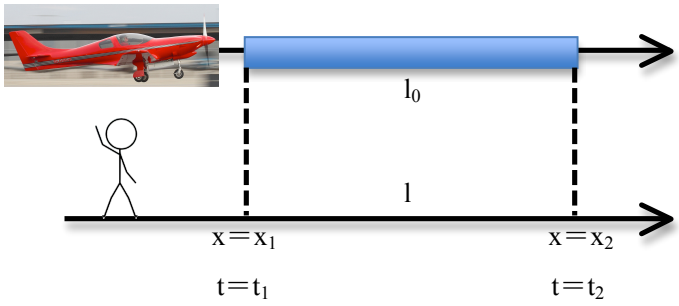
$t_2 = t_1$，$l_0 = x_2' - x_1'$，$l = x_2 - x_1$ より，

$$l_0 = \gamma l$$

$\gamma > 1$ より，

$$l_0 > l$$

よって，速度 v で飛ぶ飛行機の中の長さ l_0 の棒は，地上では縮んで見える！



■地上の棒を，飛行機の中の B が観測する

A の棒の左端の座標を x_1，右端の座標を x_2 とすると，A が地上で測った棒の長さは，

$$l_0 = x_2 - x_1$$

である。

ここで，飛行機の中の B が地上の棒を観測する。棒の左端が座標 x_1'に来たときの時刻を t_1'，その同時刻($t_2' = t_1'$)に棒の右端の座標を観測すると x_2'であったとすると，B が観測する棒の長さは，

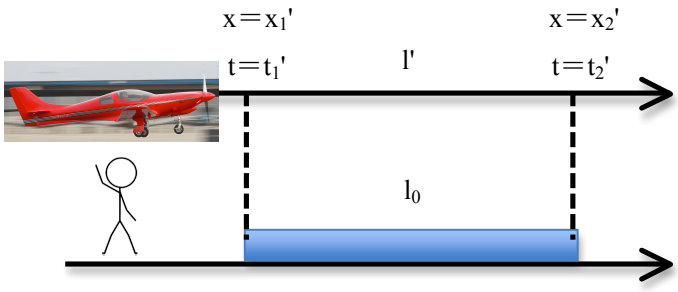
$$l' = x_2' - x_1'$$

である。

ここで，飛行機の中の B からは，地上の A は速度−v で運動しているように見えるので，(R1)より，

$$x_1 = \gamma (x_1' + c\beta t_1') \cdots ③$$

$$x_2 = \gamma (x_2' + c\beta t_2') \cdots ④$$



④−③より，

$$x_2 - x_1 = \gamma \{(x_2' - x_1') + c\beta (t_2' - t_1')\}$$

$t_2' = t_1'$，$l_0 = x_2 - x_1$，$l' = x_2' - x_1'$より，

$$l_0 = \gamma l'$$

$\gamma > 1$ より，

$$l_0 > l'$$

よって，地上の長さ l_0 の棒は，速度 v で飛ぶ飛行機の中では縮んで見える！

ここで，飛行機から見れば地上は速度−v で動いていることになる。

以上より，

動く物体は縮んで見える！

2. 時間について

2 つの慣性系 K，K'があり，K に対して相対速度 v で K'が動いているとする。K で時間が t_1 から t_2 に進んだとき，K'の座標 x'における時間が t_1'から t_2'に進んだとすると，(R2)より，

$$t_1 = \gamma \left(t_1' + \frac{\beta}{c} x'\right) \cdots ⑤$$

$$t_2 = \gamma \left(t_2' + \frac{\beta}{c} x'\right) \cdots ⑥$$

⑥−⑤より，

$$t_2 - t_1 = \gamma (t_2' - t_1')$$

$v \neq 0$ のときは，$\gamma > 1$ より，

$$t_2 - t_1 > t_2' - t_1'$$

よって，K の時間経過は，相対速度 v で動く K'の時間経過より長い！

つまり，

動いている慣性系では，時間は遅れる！

［問 4］ $\beta = \frac{v}{c} = 0.5$ のとき，K で 10 年が経過したときには，K'では何年が経過するか。

逆に，K'を基準にして考える。K の座標 x における時間が t_1 から t_2 に進んだとき，K'の時間が t_1'から t_2'に進んだとすると，(L2)より，

$$t_1' = \gamma\left(t_1 - \frac{\beta}{c}x\right)\cdots⑦$$

$$t_2' = \gamma\left(t_2 - \frac{\beta}{c}x\right)\cdots⑧$$

⑧−⑦より，

$$t_2' - t_1' = \gamma\,(t_2 - t_1)$$

$v \neq 0$ のときは，$\gamma > 1$ より，

$$t_2' - t_1' > t_2 - t_1$$

よって，K'の時間経過は，相対速度−v で動く K の時間経過より長い！

つまり，動いている慣性系では，時間は遅れる！

［問 5］以上から，慣性系 K から K'を見ると K'の時間が遅れ，K'から K を見ると K の時間が遅れることになる。これは矛盾しているのではないか？一体，どちらの時間が遅れるのか？

［問 6］＊　双子がいて，兄が光速に近い超高速の宇宙船で宇宙に飛び立ち，弟は地球に残ったとする。相対的に若くなるのは，兄か弟か？

［問 7］＊　兄が宇宙に飛び立ったままでは，どちらが若くなるかはわからないので，兄はあるときに方向転換して地球に戻ってきた。相対的に若くなるのは，兄か弟か？

*は，ミンコフスキー空間の知識が必要で難しい。

3. 時間の遅れの証拠

ローレンツ変換から，「動いている慣性系では時間が遅れる」ことを導いた。物理学では，その理論が正しいかどうかは，実験結果を明確に説明できるかどうかで判断する。その説明は，言葉による定性的な説明ではなく，実験による測定データと理論による計算結果がピタリと一致する定量的な説明でなければならない。［問 5］〜［問 7］をぱっと見ると，時間の遅れは矛盾を含んでいて，この理論は本当に正しいのかと疑ってしまう。

その疑いを晴らしたのが，宇宙線の観測結果である。宇宙線は，太陽の表面の爆発などで発生した高速度の粒子であり，次の 2 種類がある。

1 次宇宙線：約 90%が陽子，10%弱がアルファ粒子(ヘリウムの原子核)

2 次宇宙線：1 次宇宙線が地球の大気圏の原子と衝突し発生する，中間子やミュー粒子

この中のミュー粒子は，$1cm^2$ 当たり 1 分間に 1 個の割合で地表まで到達する。観測結果によると，ミュー粒子は 2.2 μ s(マイクロ秒＝10^{-6}s)で崩壊して，別の粒子に変わることがわかった。したがって，光速の 99.5%の速度(0.995c km/s)で地上 6km から降り注ぐミュー粒子は，単純には，

30 万 km/s×0.995×2.2 μ s＝0.6567km･･･(*)

しか進むことができない。これでは，地上 6km から地表まで到達できない！

［問 8］(*)の計算は，古典力学における計算である。特殊相対性理論による時間の遅れを考慮した計算を行い，ミュー粒子が地表に到達できることを示せ。

§8　4 次元時空

ローレンツ変換

$$x' = \gamma (x - c\beta t) \quad \cdots(L1)$$

$$t' = \gamma \left(t - \frac{\beta}{c} x\right) \quad \cdots(L2)$$

を見ると，x', t'ともに x と t の両方に依存していることがわかる。つまり，空間と時間は独立したものではなく，この 2 つの間には密接な結び付きが存在するのである。

そこで，1908 年にドイツの数学者ミンコフスキー(1864～1909)は，空間と時間を統一的に扱うこと，すなわち，3 次元の空間と 1 次元の時間を一体化した 4 次元時空で相対性理論を考えることを提唱した。すべての事象は場所と時間で指定されるので，x，y，z，t の 4 変数が必要なのである。私たちは，4 次元世界(4 次元空間ではない！)に住んでいるのだ。

ここで，(L1)，(L2)の逆変換

$$x = \gamma (x' + c\beta t') \quad \cdots(R1)$$

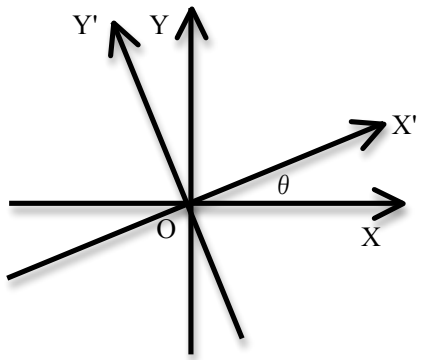
$$t = \gamma \left(t' + \frac{\beta}{c} x'\right) \quad \cdots(R2)$$

を見ると，ある式に似ていることに気づく。

直交する X 軸，Y 軸で定まる座標平面を，原点を中心に θ だけ回転した座標平面の軸を X'軸，Y'軸とする。ある点の XY 座標を(x，y)，X'Y'座標を(x'，y')とすると，

$$\begin{cases} x = x'\cos\theta - y'\sin\theta \\ y = x'\sin\theta + y'\cos\theta \end{cases} \quad \cdots(8-1)$$

となる。



［問 9］(8−1)を証明せよ。

(R1)，(R2)より，

$$\begin{cases} x = \gamma x' + c\beta\gamma t' \\ t = \dfrac{\beta\gamma}{c} x' + \gamma t' \end{cases} \quad \cdots(8-2)$$

ここで，ミンコフスキーは，

$$t = \frac{i}{c}\tau, \quad t' = \frac{i}{c}\tau' \quad (i = \sqrt{-1}) \cdots(☆)$$

と置き換えた。すると(8-2)は，

$$\begin{cases} x = \gamma x' - (-i\beta\gamma)\tau' \\ \tau = (-i\beta\gamma)x' + \gamma\tau' \end{cases} \quad \cdots(8-3)$$

となる。

$$\gamma^2 + (-i\beta\gamma)^2 = \gamma^2(1-\beta^2) = 1$$

より，

(☆)については，次のような説明ができるか。

(8-2)を $t = T\tau$，$t' = T\tau'$と変数変換して，(8−1)の形にしたい。(8−2)に代入すると，

$$\begin{cases} x = \gamma x' + c\beta\gamma T\tau' \\ T\tau = \dfrac{\beta\gamma}{c} x' + \gamma T\tau' \end{cases} \Leftrightarrow \begin{cases} x = \gamma x' + c\beta\gamma T\tau' \\ \tau = \dfrac{\beta\gamma}{Tc} x' + \gamma\tau' \end{cases}$$

よって，$-c\beta\gamma T = \dfrac{\beta\gamma}{Tc}$ であればよい。

すなわち，$T^2 = -\dfrac{1}{c^2}$ より，$T = \dfrac{i}{c}$

$\gamma = \cos\theta$，$-i\ \beta\ \gamma = \sin\theta$ ･･･(8−4)

とおける。ただし，$\gamma > 1$ より，θ は虚数の角度である。

よって，(8−3)は，

$$\begin{cases} x = x'\cos\theta - \tau'\sin\theta \\ \tau = x'\sin\theta + \tau'\cos\theta \end{cases} \quad \cdots(8-5)$$

となる。

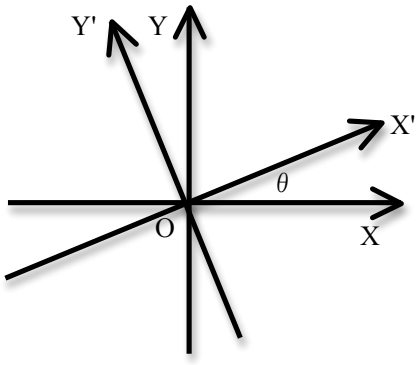
したがって，

慣性系 K：(x，y，z，τ)

慣性系 K’：(x'，y'，z'，τ')

とすると，K を K'に座標変換することは，K の座標系 XT を原点を動かさずに θ 回転させた座標系 X'T'を考えることになる。つまり，

ローレンツ変換は回転変換である！



このとき，(8−4)より，

$$\tan\theta = -i\ \beta = -i\cdot\frac{v}{c} \cdots(8-6)$$

よって，回転角 θ は相対速度 v に依存して決まる。

［研究］ 虚数の角度を持つ(8−5)を，違う方法で導く。

(8−3)において，

$\gamma^2 - (-\beta\ \gamma)^2 = \gamma^2(1-\beta^2) = 1$

より，次のように定義される双曲線関数

$$\cosh\phi = \frac{e^{\phi}+e^{-\phi}}{2} \quad \text{(ハイパボリックコサイン)}$$

$$\sinh\phi = \frac{e^{\phi}-e^{-\phi}}{2} \quad \text{(ハイパボリックサイン)} \quad \text{(e は自然対数の底で，e=2.71828･･･)}$$

を用いて，

$\gamma = \cosh\phi$，$-\beta\ \gamma = \sinh\phi$ ･･･(8−7)

とおける。

［問 10］$\cosh^2\phi - \sinh^2\phi = 1$ を証明せよ。

ここで，関数 f(x)を冪関数 x^n (n＝0，1，2，3，･･･)で表すことを考える。

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + \cdots + a_nx^n + \cdots \quad (8-8)$$

とおく。a_n（n＝0，1，2，3，･･･）を求めればよいので，(*)は無限個の和だけれど気にしないで微分する。

$\frac{d}{dx}x^n = nx^{n-1}$

であるから，

$f'(x)=1\cdot a_1+2a_2x^1+3a_3x^2+4a_4x^3+5a_5x^4+\cdots+na_nx^{n-1}+\cdots$

$f''(x)=2\cdot1\cdot a_2+3\cdot2a_3x^1+4\cdot3a_4x^2+5\cdot4a_5x^3+\cdots+n(n-1)a_nx^{n-2}+\cdots$

$f'''(x)=3\cdot2\cdot1\cdot a_3+4\cdot3\cdot2a_4x^1+5\cdot4\cdot3a_5x^2+\cdots+n(n-1)(n-2)a_nx^{n-3}+\cdots$

$f^{(4)}(x)=4\cdot3\cdot2\cdot1\cdot a_4+5\cdot4\cdot3\cdot2a_5x^1+\cdots+n(n-1)(n-2)(n-3)a_nx^{n-4}+\cdots$

$f^{(5)}(x)=5\cdot4\cdot3\cdot2\cdot1\cdot a_5+\cdots+n(n-1)(n-2)(n-3)(n-4)a_nx^{n-3}+\cdots$

・・・・・・・・・

これらの式に，x＝0 を代入すると，

$f(0)=a_0$　　$f'(0)=1\cdot a_1$　　$f''(0)=2\cdot1\cdot a_2$

$f'''(0)=3\cdot2\cdot1\cdot a_3$　　$f^{(4)}(0)=4\cdot3\cdot2\cdot1\cdot a_4$　　$f^{(5)}(0)=5\cdot4\cdot3\cdot2\cdot1\cdot a_5$

・・・・・・・・・

よって，

$a_0=f(0)$　　$a_1=\dfrac{f'(0)}{1!}$　　$a_2=\dfrac{f''(0)}{2!}$

$a_3=\dfrac{f'''(0)}{3!}$　　$a_4=\dfrac{f^{(4)}(0)}{4!}$　　$a_5=\dfrac{f^{(5)}(0)}{5!}$

・・・・・・・・・

ゆえに，一般に，

$a_k=\dfrac{f^{(k)}(0)}{k!}$　　(k＝0，1，2，3,・・・)

よって，(8−8)は

$$f(x)=f(0)+\frac{f'(0)}{1!}x+\frac{f''(0)}{2!}x^2+\frac{f'''(0)}{3!}x^3+\frac{f^{(4)}(0)}{4!}x^4+\frac{f^{(5)}(0)}{5!}x^5+\cdots+\frac{f^{(n)}(0)}{n!}x^n+\cdots \quad (M)$$

となる。この展開式を，f(x)のマクローリン展開という。

種々の関数のマクローリン展開は，次のようになる。ただし，（　）内は収束範囲を表す。

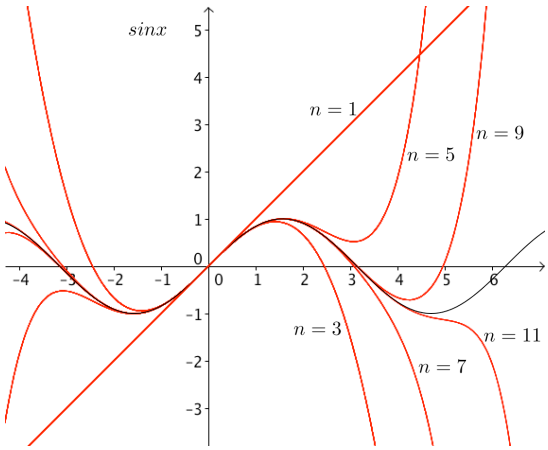
$$\sin x=x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\frac{x^9}{9!}-\cdots\cdots \qquad (-\infty<x<\infty)$$

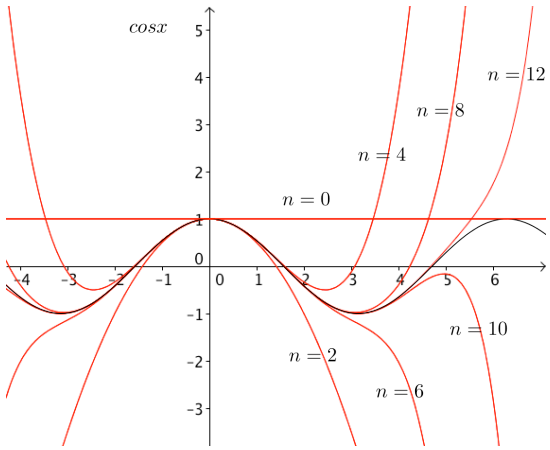
$$\cos x=1-\frac{x^2}{2!}+\frac{x^4}{4!}-\frac{x^6}{6!}+\frac{x^8}{8!}-\cdots\cdots \qquad (-\infty<x<\infty)$$

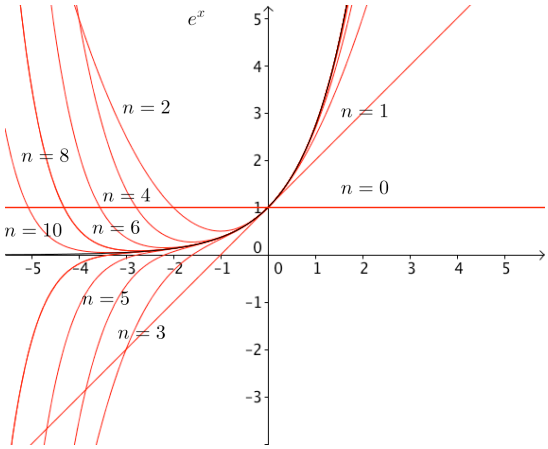
$$e^x=1+\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}+\frac{x^5}{5!}+\frac{x^6}{6!}+\frac{x^7}{7!}+\frac{x^8}{8!}+\cdots\cdots \qquad (-\infty<x<\infty)$$

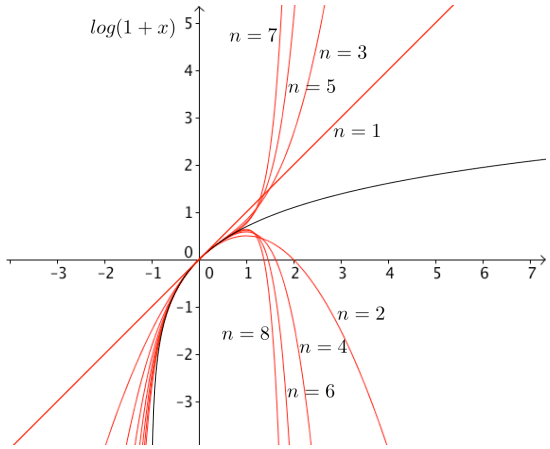
$$\log(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\frac{x^4}{4}+\frac{x^5}{5}-\frac{x^6}{6}+\cdots\cdots \qquad (-1<x<1)$$

これらのマクローリン展開のグラフを描くと，次の図のようになる。









このように，三角関数や指数関数，対数関数が冪級数で表せるのだ！

さて，スイスの天才数学者オイラー(1707～1783)は計算が大好きであり，いろいろな素晴らしい結果を得ている。

例えば，e^x のマクローリン展開

$$e^x = 1+\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}+\frac{x^5}{5!}+\frac{x^6}{6!}+\frac{x^7}{7!}+\frac{x^8}{8!}+\cdots\cdots \qquad (-\infty<x<\infty) \quad (☆)$$

において，天才オイラーは素晴らしい直観で(☆)の x に ix $(i=\sqrt{-1})$を代入した！　すると，

$$e^{ix} = 1+\frac{(ix)}{1!}+\frac{(ix)^2}{2!}+\frac{(ix)^3}{3!}+\frac{(ix)^4}{4!}+\frac{(ix)^5}{5!}+\frac{(ix)^6}{6!}+\frac{(ix)^7}{7!}+\frac{(ix)^8}{8!}+\cdots\cdots$$

$$=\left(1-\frac{x^2}{2!}+\frac{x^4}{4!}-\frac{x^6}{6!}+\frac{x^8}{8!}-\cdots\cdots\right)+i\left(x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\frac{x^9}{9!}-\cdots\cdots\right)$$

$$=\cos x+i\sin x$$

よって，次のオイラーの公式が得られる。

$$e^{ix}=\cos x+i\sin x \quad \cdots(\mathrm{E})$$

なんと，複素数の世界では，指数関数と三角関数が結びつく！

(E)において，x＝ϕ，$-\phi$とすると，

$$e^{i\phi}=\cos\phi+i\sin\phi,\quad e^{-i\phi}=\cos\phi-i\sin\phi$$

よって，複素数の世界では，次のように三角関数が指数関数で表される。

$$\cos\phi=\frac{e^{i\phi}+e^{-i\phi}}{2},\ \sin\phi=\frac{e^{i\phi}-e^{-i\phi}}{2i}\quad\cdots(8\text{−}9)$$

ゆえに，(8−7)より，

$$\gamma=\cosh\phi=\frac{e^{-i(i\phi)}+e^{i(i\phi)}}{2}=\cos(i\phi)$$

$$-i\ \beta\ \gamma=i\sinh\phi=i\cdot\frac{e^{-i(i\phi)}-e^{i(i\phi)}}{2}=\frac{e^{i(i\phi)}-e^{-i(i\phi)}}{2i}=\sin(i\phi)$$

よって，(8−3)は，

$$\begin{cases}x=x'\cos(i\phi)-\tau'\sin(i\phi)\\ \tau=x'\sin(i\phi)+\tau'\cos(i\phi)\end{cases}\quad\cdots(8\text{−}9)$$

となり，ローレンツ変換は座標回転として表せる。ただし，回転角は虚数の角$i\phi$である(虚数の角はイメージするのは難しいが･･･)。

§9　相対性理論における速度の合成

古典物理学におけるガリレイ変換では，速度の合成は簡単で，例えば，50km/h で動いている電車の中を 2km/h で歩く人の地面に対する相対速度は，

50km/h＋2km/h＝52km/h

と単純に 2 つの速度 V_1 と V_2 をたして，V_1+V_2 とすればよい。

ところが，速度が光速に近づくと，ガリレイ変換ではおかしなことになる。例えば，

V_1＝0.5c，V_2＝0.8c とすると，V_1+V_2＝1.3c

となって，光速度 c を超えてしまう。

そこで，ローレンツ変換を用いて相対性理論における速度の合成を考える。

慣性系 K_0 に対して x 軸の正の方向に速度 V_1 で動く慣性系 K_1 があり，K_1 に対して x 軸の正の方向に速度 V_2 で動く慣性系 K_2 があるとする。このとき，K_2 の K_0 に対する相対速度を，ローレンツ変換を用いて求めるには，ローレンツ変換を 2 回行えばよい。ここで，ローレンツ変換は座標回転として表せたことを利用する。

合成する速度を$\frac{V_1}{c}$，$\frac{V_2}{c}$とすると，それぞれの回転角との関係は，(8−6)より，

$$\tan\theta_1=-i\cdot\frac{V_1}{c},\ \tan\theta_2=-i\cdot\frac{V_2}{c}\quad(\theta_1,\ \theta_2\text{は虚数の角度})$$

2 回の座標回転を行うので，角度$\theta_1+\theta_2$に対応する速度 v を求めればよい。

$$\tan(\theta_1+\theta_2)=\frac{\tan\theta_1+\tan\theta_2}{1-\tan\theta_1\tan\theta_2}=\frac{-i\left(\frac{V_1}{c}+\frac{V_2}{c}\right)}{1+\frac{V_1}{c}\cdot\frac{V_2}{c}}=-\frac{i}{c}\cdot\frac{V_1+V_2}{1+\frac{V_1V_2}{c^2}}$$

よって，$\frac{V_1}{c}$，$\frac{V_2}{c}$ の合成速度 v は，

$$v=\frac{V_1+V_2}{1+\frac{V_1V_2}{c^2}} \cdots(9-1)$$

となる。特に，$V_1=V_2=V$ のときは，合成速度は，

$$v=\frac{2V}{1+\frac{V^2}{c^2}} \cdots(9-2)$$

である。

［問 11］(9−2)において，V を限りなく光速度 c に近づけると，v はどのような速度に近づくか。
また，合成速度 v は光速度 c を超えないことを証明せよ。

§10　相対性理論における保存則

(8−5)より，

$$\begin{aligned} x&=x'\cos\theta-\tau'\sin\theta \\ \tau&=x'\sin\theta+\tau'\cos\theta \end{aligned} \quad \cdots(8-5)$$

であるから，

$$x^2=x'^2\cos^2\theta-2x'\tau'\sin\theta\cos\theta+\tau'^2\sin^2\theta$$
$$\tau^2=x'^2\sin^2\theta+2x'\tau'\sin\theta\cos\theta+\tau'^2\cos^2\theta$$

よって，

$$x^2+\tau^2=x'^2+\tau'^2$$

これと，$y^2=y'^2$，$z^2=z'^2$ より，

$$x^2+y^2+z^2+\tau^2=x'^2+y'^2+z'^2+\tau'^2 \cdots(10-1)$$

ここで，2 次元ユークリッド平面や，3 次元ユークリッド空間における距離の拡張として，

$x^2+y^2+z^2+\tau^2$: 4 次元世界における 2 つの事象の「間隔」または「世界距離」

と定義すると，(10−1)は，2 つの事象の「間隔」は，慣性系 K，K'のどちらで観測しても変わらないことを意味している。

すなわち，2 つの慣性系 K，K'では，長さや時間の測定結果は一致しないが，物理法則の記述や 2 つの事象の「間隔」は一致するのである。言い換えると，

長さや時間は不変量ではないが，2 つの事象の「間隔」は不変量

となる。

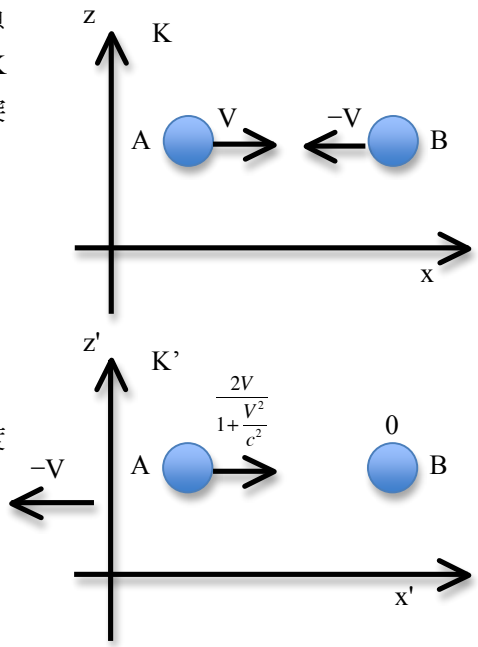
ニュートン力学では，

質量保存の法則，運動量保存の法則，エネルギー保存の法則など

の重要な保存則が成立していた。そこで，それらに対応する相対性理論における保存則を考える。つまり，保存則を 4 次元時空に拡張するのである。

1. 運動量保存の法則

2 つの慣性系 K，K'があり，K'は K に対して速度−V で x 軸の負の方向に動いているとする。2 つの質量 m の球 A，B を考え，K において A は速度 V で，B は速度−V で動くのが観測され，衝突後は合体して静止したとする。



K において運動量保存の法則を適用すると，

(運動量)＝(質量)×(速度)

より，

$$mV+m(-V)=0$$

となる。

次に，K'から観測する。衝突前の K'における A の速度は，速度の合成の公式(9−2)より，

$$\frac{2V}{1+\frac{V^2}{c^2}}$$

である。一方で，B の速度は明らかに 0 である。よって，衝突前の運動量の合計は，

$$m\times\frac{2V}{1+\frac{V^2}{c^2}}+m\times 0=\frac{2mV}{1+\frac{V^2}{c^2}}\cdots(10-2)$$

また，衝突後に合体した A と B の速度は，K'から見た K の相対速度なので V である。よって，衝突後の運動量は，

$$2m\times V=2mV\cdots(10-3)$$

したがって，K'から見た運動量保存の法則を書くとすれば，(10−2)，(10−3)より，

$$\frac{2mV}{1+\frac{V^2}{c^2}}=2mV$$

となるが，これは成立しない！つまり，ニュートン力学の運動量保存の法則は成り立たなくなった。これでは困るので，修正を行う。

速度について相対性理論における考えを取り入れていることは，(10−2)からわかる。ところが，運動量の要素の 1 つである質量には，相対性理論による修正は行われていない。つまり，

物理の基本単位である MKS(CGS)のうち，K(G)は手つかず

であった。これが，運動量保存の法則が成り立たなくなった理由だろう。

そこで，絶対時間・絶対空間が存在しないのと同じく，質量について，

ある慣性系で測定した物体の速度 v に依存して，質量は変化する

と考える。つまり，質量は定数 m ではなく，物体の速度 v の関数 m(v)であると仮定する。

K'における A の速度を，

$$v=\frac{2V}{1+\frac{V^2}{c^2}}\cdots(10-4)$$

とおくと，K'における衝突前の質量は，

$$m(v)+m(0)$$

であり，衝突後の質量も速度に依存するので，それを M(V)とおくと，

$$m(v)+m(0)=M(V)\cdots(10-5)$$

となる。これが，相対性理論における質量保存の法則となる。

すると，(10−2)，(10−3)は，

$$m(v)\times\frac{2V}{1+\frac{V^2}{c^2}}+m(0)\times 0=M(V)\times V\cdots(10-6)$$

と修正される。これが，相対性理論における運動量保存の法則となる。

(10−5)を(10-6)に代入して，

$$\frac{2m(v)V}{1+\frac{V^2}{c^2}}=\{m(v)+m(0)\}V$$

$$m(v)\left(1-\frac{V^2}{c^2}\right)=m(0)\left(1+\frac{V^2}{c^2}\right)$$

よって，

$$m(v)=\frac{1+\frac{V^2}{c^2}}{1-\frac{V^2}{c^2}}m(0)\cdots(10-7)$$

ここで，$\gamma=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$ を用いて書き直すために，(10-4)より，

$$1-\left(\frac{v}{c}\right)^2=1-\left(\frac{\frac{2V}{c}}{1+\frac{V^2}{c^2}}\right)^2\cdots(10-8)$$

$1-\left(\frac{v}{c}\right)^2=\frac{1}{\gamma^2}$ であるから，(10−8)より，

$$\frac{1}{\gamma^2}=\frac{\left(1+\frac{V^2}{c^2}\right)^2-4\left(\frac{V}{c}\right)^2}{\left(1+\frac{V^2}{c^2}\right)^2}=\frac{\left(1-\frac{V^2}{c^2}\right)^2}{\left(1+\frac{V^2}{c^2}\right)^2}$$

$\gamma>0$ より，

$$\gamma=\frac{1+\frac{V^2}{c^2}}{1-\frac{V^2}{c^2}}\cdots(10-9)$$

(10−7)，(10−9)より，

$$m(v)=\gamma\, m(0)=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}m(0)\cdots(10-10)$$

(10−10)の m(v)が，運動量保存の法則を満たす質量となる。m(0)は速度が 0 のときの質量だから，静止質量と呼び，m_0 で表す。

以上より，相対性理論における運動量 p は，

$$p=m(v)v=\gamma\, m_0v=\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}m_0v\cdots(10-11)$$

と定義すればよく，これで運動量保存の法則が成立することになる。

［問 12］(10−10)より，速度 v のときの質量 m(v)と静止質量 m_0 の大小関係を調べよ。また，速度 v が限りなく光速度 c に近づくとき，質量 m(v)はどのようになるか調べよ。

［問 13］(10−11)より，速度 v が光速度 c に比べて非常に小さいとき(v<<c)，運動量 p はどうなるか。

2. 相対性理論における力

※これ以降は，微積分の知識と計算力が必要である。

ニュートン力学においては，力を F，質量を m，速度を v，加速度を α，運動量を p とすると，

$$F=m\alpha,\quad \alpha=\frac{dv}{dt},\quad p=mv$$

であるから，

$$\frac{dp}{dt}=m\frac{dv}{dt}=m\alpha=F$$

すなわち，

$$F=\frac{dp}{dt}\cdots(10-12)$$

であった。これを相対性理論における力に拡張するために，(10−12)に(10−11)を代入する。

$$F=\frac{dp}{dt}=\frac{d}{dt}\frac{m_0v(t)}{\sqrt{1-\frac{v^2(t)}{c^2}}}\cdots(10-13)$$

ここで，v(t)<<c のときは，(10−13)は，ニュートン力学の力と一致する。

簡単のために v(t)＝v と書いて，(10−13)の右辺を計算する。

$$F=\frac{m_0}{\sqrt{1-\frac{v^2}{c^2}}}\cdot\frac{dv}{dt}+m_0v\frac{d}{dt}\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$$

$$= \frac{m_0}{\sqrt{1-\frac{v^2}{c^2}}} \cdot \frac{dv}{dt} + \mathrm{m_0 v} \left\{ -\frac{1}{2}\left(1-\frac{v^2}{c^2}\right)^{-\frac{3}{2}} \cdot \left(-\frac{2v}{c^2}\right) \cdot \frac{dv}{dt} \right\}$$

$$= \frac{m_0}{\sqrt{1-\frac{v^2}{c^2}}} \cdot \frac{dv}{dt} + \mathrm{m_0 v} \cdot \frac{v}{c^2} \cdot \frac{1}{\sqrt{1-\frac{v^2}{c^2}}\left(1-\frac{v^2}{c^2}\right)} \cdot \frac{dv}{dt} \cdots (10\text{−}14)$$

ここで，上の計算より，

$$\frac{d}{dt}\frac{1}{\sqrt{1-\frac{v^2}{c^2}}} = \frac{v}{c^2} \cdot \frac{1}{\sqrt{1-\frac{v^2}{c^2}}\left(1-\frac{v^2}{c^2}\right)} \cdot \frac{dv}{dt} \cdots (10\text{−}15)$$

よって，

$$\frac{1}{\sqrt{1-\frac{v^2}{c^2}}} \cdot \frac{dv}{dt} = \frac{c^2}{v}\left(1-\frac{v^2}{c^2}\right) \cdot \frac{d}{dt}\frac{1}{\sqrt{1-\frac{v^2}{c^2}}} \cdots (10\text{−}16)$$

(10−14)の第 1 項に(10−16)，第 2 項に(10−15)を代入すると，

$$\mathrm{F} = \frac{m_0 c^2}{v}\left(1-\frac{v^2}{c^2}\right) \cdot \frac{d}{dt}\frac{1}{\sqrt{1-\frac{v^2}{c^2}}} + \mathrm{m_0 v} \cdot \frac{d}{dt}\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$$

$$= \left\{ \frac{m_0 c^2}{v}\left(1-\frac{v^2}{c^2}\right) + m_0 v \right\} \cdot \frac{d}{dt}\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$$

$$= \frac{m_0 c^2}{v} \cdot \frac{d}{dt}\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$$

よって，

$$\mathrm{F} = \frac{1}{v(t)} \cdot \frac{d}{dt}\frac{m_0 c^2}{\sqrt{1-\frac{v^2(t)}{c^2}}} \cdots (10\text{−}17)$$

これが，相対性理論における力である。

§11　$\mathrm{E}=\mathrm{mc}^2$

次に，相対性理論におけるエネルギーはどのように書けるかを考える。

ニュートン力学における力を F，エネルギーを E，力 F で物体を x だけ動かしたときの仕事を W とすると，W は E と等価なので，

$$\mathrm{W} = \mathrm{Fx} \quad \Leftrightarrow \quad \mathrm{E} = \mathrm{Fx}$$

よって，

$$\frac{dE}{dt} = \frac{dF}{dt} \cdot \mathrm{x} + \mathrm{F} \cdot \frac{dx}{dt} = \frac{dF}{dt} \cdot \mathrm{x} + \mathrm{Fv}$$

ここで，F が一定なら $\frac{dF}{dt}=0$ より，

$$\frac{dE}{dt}=\mathrm{Fv}\cdots(11-1)$$

したがって，相対性理論におけるエネルギーE の時間変化は，(11−1)に(10−17)を代入して得られる。すなわち，

$$\frac{dE}{dt}=\mathrm{Fv(t)}=\frac{d}{dt}\frac{m_0c^2}{\sqrt{1-\frac{v^2(t)}{c^2}}}$$

よって，微分されている部分を比較し，(10−10)も考慮すると，E は次のように表される。

$$\mathrm{E}=\frac{m_0c^2}{\sqrt{1-\frac{v^2(t)}{c^2}}}=\mathrm{m(v)c^2}\cdots(11-2)$$

これが，相対性理論におけるエネルギーE である。

(11−2)を簡潔に書くと，

$$\mathrm{E}=\mathrm{mc^2}\cdots(11-3)\quad\leftarrow\quad\text{エネルギーと質量は同じ 1 つの存在である！！}$$

となり，有名なアインシュタインのエネルギー公式が得られた！

ここで，x<<1 のときの近似公式

$$\frac{1}{\sqrt{1-x}}=(1-x)^{-\frac{1}{2}}\fallingdotseq 1+\frac{1}{2}\mathrm{x}$$

を利用すると，$\frac{v^2(t)}{c^2}$<<1 であるから，(11−2)より，

$$\mathrm{E}=\frac{m_0c^2}{\sqrt{1-\frac{v^2(t)}{c^2}}}\fallingdotseq \mathrm{m_0c^2}\left(1+\frac{1}{2}\cdot\frac{v^2(t)}{c^2}\right)=\mathrm{m_0c^2}+\frac{1}{2}\mathrm{m_0v^2(t)}\cdots(11-4)$$

となる。

(11−4)の第 2 項は，ニュートン力学における運動エネルギーと同じである。

第 1 項は，v(t)＝0 のとき，すなわち運動していないときも物体が持っているエネルギーで，ポテンシャルエネルギー(静止エネルギー)という。

［問 14］(11−3)を利用して，1g の物質が持つエネルギーをジュール J(kgm2/s2)に換算せよ。

［問 15］1g の物質が持つエネルギーを，100 万 kW の発電所が生み出そうとすれば，どれくらいの時間が必要か。ただし，1kW×1s＝1J である。

【参考文献】

第 1 章

加藤文元(2007)『物語　数学の歴史　正しさへの挑戦』中央公論新社(中公新書)

上野健爾(2013)『円周率が歩んだ道』岩波書店(岩波現代全書)

ファン・デル・ヴェルデン(訳：加藤文元，鈴木亮太郎)(2006)『ファン・デル・ヴェルデン 古代文明の数学』日本評論社

第 2 章

ジェフリー・S・ローゼンタール(訳：柴田裕之)(2012)『運は数学にまかせなさい　確率・統計に学ぶ処世術』早川書房(ハヤカワ文庫)

小島寛之(2004)『確率的発想法~数学を日常に活かす』NHK 出版

サイモン・シン(訳：青木薫)(2001)『暗号解読　ロゼッタストーンから量子暗号まで』新潮社

第 3 章

山口栄一(2014)『死ぬまでに学びたい 5 つの物理学』筑摩書房

リリアン・R・リーバー(訳：水谷淳)(2012)『数学は相対論を語る』ソフトバンククリエイティブ

スティーブン・L・マンリー(訳：吉田三知世)(2011)『アメリカ最優秀教師が教える相対論＆量子論』講談社(ブルーバックス)

竹内淳(2014)『高校数学でわかる相対性理論』講談社(ブルーバックス Kindole 版)

LADy SCIENCE BOOKLET 1
文化としての数学を

2015 年 3 月 27 日発行
奈良女子大学　理系女性教育開発共同機構
CORE of STEM
Collaborative Organization for Research in women's Education of
Science, Technology, Engineering, and Mathematics
〒630-8506　奈良市北魚屋東町
コラボレーションセンター　Z207
TEL.&FAX 0742-20-3266
ladyscience@cc.nara-wu.ac.jp