

数学入門資料

1 最初に

歴史に記録が残っていないような昔でも人は「一つ、二つ...」と物を数えていたことは間違いないでしょう。このように1, 2, 3, ... とものを数えるときに用いる数を**自然数**といいます。紀元前17世紀のエジプトでは自然数より更に進んで分数を使った計算が行われていました。但し古代のエジプト人・(下で述べる)ギリシャ人には、まだ0と言う考えはありませんでした。

0を用いた数字の記法は6世紀前後のインドに始まると言われていますが、0は「何も無いものがあると見なす」という観点よりは、むしろ1, 2, ..., 9, 10, 11, ..., 99, 100, 101, ... と言った具合に、0から9までの数字だけを用いて全ての自然数を表す、「位取り記数法」に利用されたことがその有用性にとっては大きな役目を果たしました。つまりこのような記法によっていくらかでも大きな数でも簡単に記述することができ、計算も(筆算などを用いて)簡単にできるようになったのです。

負の数の導入とその加法・減法の法則の発見は古代中国でなされました。中国最古の数学書と呼ばれている「九章算術」では、「負数」は金額の不足を表す数をあらわしていました。(「負」という漢字はもともと「借り」(負債)を意味するそうです。)この負数の概念がインドに渡り、更にヨーロッパまで伝えられましたが、ヨーロッパでは14世紀になってようやく一部の学者が負の数を認めるようになりました。(多くの学者は負の数を「うその数」と呼んでいました。実際のところ、負の数どうしの積、例えば $(-3) \times (-2)$ 、の意味付けには当惑と疑いを向けられていました。)しかしながら17世紀以降、数学、力学、天文学が大きく発展し、その過程で負の数を認めると計算が著しく軽減されるので役に立つものであると言う認識と同時にまた様々な計算と矛盾することも無いことが明らかになって、次第に数学に根付いてきました。(自然数に0を付け加えて、さらに負の数にまで拡大したものの全体 $\{\dots, -2, -1, 0, 1, 2, \dots\}$ を**整数**と言います。)

紀元前6世紀頃、ピタゴラス(Pythagoras, B.C. 560頃 ~ 480頃)に代表される古代ギリシャでは幾何学が盛んでした。当時は自然数や自然数の比(分数)のみを数学の対象としていました。ところがピタゴラス(学派の人々)は正方形の対角線と一辺の比が「分数で表すことのできない数」(**無理数**)になることを発見していたのですがこのことを公に認めると自分達の数学が否定されると恐れ、その存在をひた隠しにしていたそうです。このような自然数に対する愛着は17世紀になってもまだ続いていたようです。(例えば19世紀のドイツの数学者クロネッカー(1823 ~ 1891)は「自然数は神が創りたもうた。その他の数は人の為せる業(わざ)である。」と言っています。)17世紀のフランスの哲学者デカルト(Descartes, 1596 ~ 1650)は「数と量は一体のもの」という認識をし分数や無理数も分数や無理数も自然数と同じように計算ができること明らかにしました。

このように数学の発展には、多くの人たちの努力と試行錯誤と長い時間がその背景にあります。この講義ではこのような数学が発展してゆく姿を念頭において数の概念から始まって暗号理論についてまで紹介をしたいと思います。

2 数学の論理

2.1 ギリシャの論理学

「証明」等で用いられる数学における議論そのものについての体系的な研究は古代ギリシャ人、特にアリストテレスによって行われました。アリストテレスはまず

「論理的な」推論と言うのは「主張」の列から構成されていて、この列に含まれるそれぞれの主張は、その直前のいくつかの主張からある「論理規則」によって生み出されている

と考えました。(この考えは現代的な数学の観点からすると全く不十分なものです。) そして彼はこの正しい結論に到達される為に使われる論理規則を列挙することを考えました。そのためには彼は、先ず上記の「主張」とは

主語とこの主語に帰結される性質(述語)という2つの側面からなる命題(:正しいかそうでないかが確定する文書)(…このような命題のことを「主語・述語命題」と呼びます)

であると決めました。

主語述語命題の例

アリストテレスは人間である。

全ての人間は死すべきものである。

アリストテレスが正しい推論を構成するために従わなければならないパターンとして考えた論理的な規則は「三段論法」として知られています。これは二つの主張から一つの主張を導き出す為の規則で例えば：

全ての人間は死すべきものである

ソクラテスは人間である

ソクラテスは死すべきものである。

がそれにあたります。このソクラテスの例はまったく自明なものですがアリストテレスはこの例にとどまらずこれ以外の三段論法のパターンを研究しました。以下彼の仕事について見てゆくことにします。

任意の主語・述語命題の主語を S 、述語を P とあらわします。このとき、

「 S は P である。」

「 S は P でない。」

のように、述語は命題の中で肯定的にも否定的にも使うことができます。さらに主語は「すべての S 」とか「ある S 」の形で表すことで「量を定める」(量化する)ことができます。主語を量化する二種類の方法を肯定的な述語と否定的な述語を組み合わせることによって、次の四種類の主語・述語命題が得られます。

すべての S は P である (All S is P)
すべての S は P でない (All S is not P)
ある S は P である (Some S is P)
ある S は P でない (Some S is not P)

ここでこれらの文章を

SaP : All S is P
 SeP : All S is not P
 SiP : Some S is P
 SoP : Some S is not P

のように省略した形であらわすことにします。以下でこの記述法を用いて三段論法を分析することにします。三段論法というのは「前提」とよばれる二つの初期命題と、これらの二つの前提から規則に従って導かれる結論からなっています。もし S と P をこの結論の中にある主語と述語だとすると、推論が成立するためには前提の中に S , P とは別の第三の量が含まれていることが必要となります。いま、この第三の量を M とかくことにします。

たとえば

全ての人間は死すべきものである
ソクラテスは人間である
ソクラテスは死すべきものである。

についていうと、「ソクラテス」が S , 「死すべきもの」が P , そして「人間」が M となります。上の記号を使えばこの三段論法は

MaP
 SaM
 SaP

とかけます。ここで通常 M と P からなる前提は「大前提」と呼ばれ、最初に書かれます。(また S と M からなるもうひとつの前提は「小前提」と呼ばれ二番目に書かれます。) 大前提は M が先か P が先かの二通りの場合があり得、また小前提には S が先か M が先かの二通りの場合があり得ますから、三段論法には次の四種類のパターンがあることとなります。

I	II	III	IV
<i>MP</i>	<i>PM</i>	<i>MP</i>	<i>PM</i>
<i>SM</i>	<i>SM</i>	<i>MS</i>	<i>MS</i>
<i>SP</i>	<i>SP</i>	<i>SP</i>	<i>SP</i>

このそれぞれの図式で主語と述語の間には a, e, i, o の四つの文字が入りうるので全体では $4 \times 4 \times 4 \times 4 = 256$ 通りの三段論法があることがわかります。もちろんこの中には正しくない三段論法も含まれていますが、アリストテレスはこの中で正当なパターンを確定しました。アリストテレスはこの 256 個の三段論法のパターンのうちで正当なものは次の 19 個であると述べました。

I:	<i>aaa</i>	<i>eae</i>	<i>aii</i>	<i>eio</i>		
II:	<i>eae</i>	<i>aee</i>	<i>eio</i>	<i>aoo</i>		
III:	<i>aai</i>	<i>iai</i>	<i>aii</i>	<i>eaο</i>	<i>oao</i>	<i>eio</i>
IV:	<i>aai</i>	<i>aee</i>	<i>iai</i>	<i>eaο</i>	<i>eio</i>	

(実はこのリストの中には正当でない推論が二個含まれています。このミスが見つかるまでには 2000 年がかかりました。)

ベン図

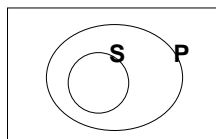
19 世紀のイギリスの数学者ジョン・ベンは三段論法の正しさを確かめるための図形的方法を考案しました。このような図は現在ベン図と呼ばれています。

ベン図の説明をするためにまず集合の説明をします。簡単に言うと「ものの集まり」のことを**集合**と呼ぶのですが、数学では特にそれに属するの、属さないのか明確なものだけを集合と呼びます。また集合に属するそれぞれのものを**要素**と呼びます。特に数学では全く要素を持たないような“集まり”も集合とみなし、このような集合のことを**空集合**と呼び ϕ という記号で表します。

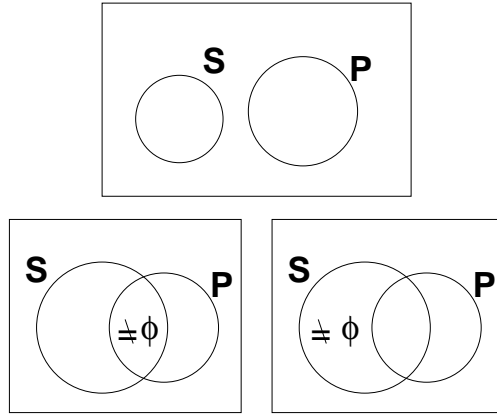
例.

例えば「背の高い人の集まり」と言うのはそれに属するの、属さないのかは明確ではありませんので集合とは呼べません。それに対して「身長 170cm 以上の人の集まり」は集合と呼ぶことができます。また「身長 100m 以上の人の集まり」は空集合となります。

さて性質 S, P で定まる集合をそれぞれ S, P と書くことにします。このとき「すべての S は P である」という命題が正しいということは次のような図で表すことができます。(このような図のことを**ベン図**と呼びます。)



また「すべての S は P でない」, 「ある S は P である」, 「ある S は P でない」はそれぞれ次のようなベン図で表されます.



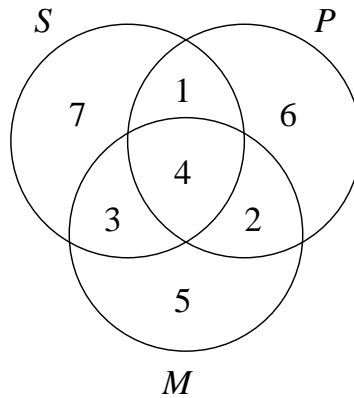
上の例

MaP

SaM

SaP

という三段論法をベン図で説明すると次のようになります.



まず「すべての M は P である」というのは 3 と 5 の領域が空集合であることを意味しています. また「すべての S は M である」というのは 1 と 7 の領域が空集合であることを意味しています. 従って二つの前提から領域 1, 3, 5, 7 が空集合ということがわかります. 従ってこれから S のすべての元は領域 4 に含まれていることがわかり, 従って S のすべての元は P に含まれている, 言い換えると SaP が正しいことがわかる, というわけです.

2.2 命題論理

古代ギリシャからおよそ 2000 年の間「推論」のパターンに対する数学的な研究はほとんど進展が見られませんでしたが、19 世紀の数学者ブール (1815~1864) はこの方面での突破口を開くことに成功しました。(ブールの仕事としては「ブール代数」による思考の把握方法が有名ですがこの講義ではブール代数については触れません。)

ブールは推論についてのパターンを見つけるためにアリストテレスが取り扱った命題よりさらに一般の命題を取り扱いました。彼は「命題」というのは「真偽が確定できる」ものであると決めました。そして命題はいくつかの厳密に記述された規則にのっとって結合されてゆくことによりより複雑な命題が構成されてゆくと考えたのでした。以下でこの結合のパターンを見てゆくことにします。

連言命題.

命題 p, q に対して「 p かつ q 」を**連言命題**と呼びます。 p と q の真偽がわかれば、連言命題「 p かつ q 」(記号で $p \wedge q$ と表します) の真偽は次のように確定します。

すなわち p と q 両方が真であれば「 p かつ q 」は真であり、 p か q (あるいはその両方) が偽であれば「 p かつ q 」は偽となります。

このことを次のような表を用いて表すことにします。(このような表のことを**真偽表**と呼びます。)

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

選言命題.

命題 p, q に対して「 p または q 」を**選言命題**と呼びます。 p と q の真偽がわかれば、選言命題「 p または q 」(記号で $p \vee q$ と表します) の真偽は次のように確定します。

すなわち p か q (あるいはその両方) が真であれば「 p または q 」は真となり、 p と q 両方が偽であれば「 p または q 」は偽となります。

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

条件命題.

命題 p, q に対して「 p ならば q 」を**条件命題**と呼びます。 p と q の真偽がわかれば、条件命題「 p ならば q 」(記号で $p \rightarrow q$ と表します) の真偽は次のように確定します。

すなわち p が真で q が偽のとき「 p ならば q 」は偽となり、それ以外のときは「 p ならば q 」は真となります。

p	q	$p \rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

否定命題.

命題 p に対して「 p でない」を**否定命題**と呼びます。 p が真のとき「 p でない」(記号で $\neg p$ と表します)は偽、 p が偽のとき「 p でない」は真となります。

p	$\neg p$
1	0
0	1

この理解によれば先に述べた三段論法は次のように解釈できます。上の条件命題の真偽を見てやると

「 p ならば q 」と p がともに真であるならば q も真である

ことがわかります。これが三段論法を含んでいるということを具体的な例で説明しましょう。例えば p として「ソクラテスは人である」、 q として「ソクラテスは死すべきものである」とすると、「ソクラテスは人であるならばソクラテスは死すべきものである」と「ソクラテスは人である」という正しい二つの前提から「ソクラテスは死すべきものである」という正しい結論が導かれることが分かりますがこれは先に述べた三段論法(の一例)に他なりません。

対偶

条件命題に関しては次のような法則が成り立ちます。

$p \rightarrow q$ が真なら $\neg q \rightarrow \neg p$ も真。また $p \rightarrow q$ が偽なら $\neg q \rightarrow \neg p$ も偽。(言い換えるとある条件命題の真偽はその対偶の真偽と一致する)

このことを証明するにはどうすればよいでしょうか？

ヒント : 「 $p \rightarrow q$ 」と「 $\neg q \rightarrow \neg p$ 」の真偽表を書いてみてください。

練習問題 「 p でなければ q である」が正しいとき、次のどれが正しいと言えるでしょうか。

1. p であれば q である
2. q であれば p でない
3. p でなければ q でない
4. q でなければ p である
5. q でなければ p でない

2.3 述語論理.

数学における証明のパターンを抽出する最後の仕上げは 19 世紀の終わりにペアノ (Giuseppe Peano, 1858~1932) とフレーゲ (Gottlob Frege, 1848-1925) によってなされました. 彼らの定式化 (述語論理) では命題の構成要素としては先に述べた命題の操作「かつ」、「または」、「～ならば」、「～でない」に加えて「すべての」と「いくつかの」という数量詞 (量化するための用語) が含まれています. (ここでは「すべての」というのは「任意のものに対して～が成り立つ」、また「いくつかの」というのは「(少なくともひとつの)～が存在する」といった言い回しで使います.) 例えば「すべての人間は死すべきものである」という命題を述語論理で書くと

任意の x に対して, x が人間であるならば, x は死すべきものである

となるのですが, 日本語で書くと論理構造がはっきりしないので, 論理学で用いられる記号を使って表現してみることにします. 述語論理では「 x は人間である」という述語を $Human(x)$ と書き, 「 x は死すべきものである」という述語を $Mortal(x)$ と書きます. また条件命題「～ならば」は矢印 \rightarrow を用いて表します. (命題論理のときと同様, 「かつ」は \wedge , 「または」は \vee , 「～でない」は \neg で表します.) さらに「すべての」は \forall を逆さまにした記号 \forall , 「いくつかの」は \exists を逆さまにした記号 \exists を用いて表します. さてこれらの記号を使うと「すべての人間は死すべきものである」という命題は

$$\forall x : Human(x) \rightarrow Mortal(x)$$

となります. 別の例として「眠らない人間が存在する」という命題を論理記号で書くと次のようになります. (ただしここでは「 x は眠る」という述語を「 $Asleep(x)$ 」と表現することにします.)

$$\exists x : Human(x) \wedge \neg Asleep(x)$$

述語論理は一見複雑そうですが, 論理の操作は非常に機械的に行うことができるという利点があります. 具体的にいうと例えば次のような規則が成り立つことが分かります.

$$\neg[P(x) \rightarrow Q(x)] = P(x) \wedge \neg Q(x)$$

$$\neg[\forall x : P(x)] = \exists x : \neg P(x)$$

これらの規則を用いると「すべての人間は死すべきものである」の否定は「ある x で, x は人間でありかつ x は死すべきものでないようなものが存在する」となることが分かります.

現在では数学の命題は, 基本的には, すべてこのような「述語論理」を用いて表現されますが, 実際に上記のような表現を用いるのはあまりにも煩雑であるので実用的には次のような簡易的な表現が用いられることが多いです.

$$\forall x(x \in \text{人間}), x \text{ は死すべきもの}$$

$\exists x(x \in \text{人間}) \text{ s.t. } x \text{ は眠らない}$

否定命題の作り方

「 $\forall x \in U, p(x)$ 」の否定は「 $p(x)$ が成り立たないような U の要素 x が存在する」となります。従って

$$\neg(\forall x \in U, p(x)) = \exists x \in U \text{ s.t. } \neg p(x)$$

が成り立ちます。また

「 $\exists x \in U \text{ s.t. } p(x)$ 」の否定は「 U に属する任意の x に対して $p(x)$ が成り立たない」ですから、

$$\neg(\exists x \in U \text{ s.t. } p(x)) = \forall x \in U, \neg p(x)$$

となります。

つまり、ごく大雑把に言うと、限定命題の否定を作るには

\forall を \exists に、 \exists を \forall に換えて、条件 $p(x)$ の代わりにその否定 $\neg p(x)$ を入れればよい。

ということになります。

例えば奈良女子大学の学生は全て女性ですが、このことを上の記号を用いて表現してやると

$$\forall x(x \in \text{奈良女子大学の学生}), x \text{ は女性}$$

となります。このときこの命題の否定（奈良女子大学の学生は全て女性，ではない）は次のようになります。

$$\exists x(x \in \text{奈良女子大学の学生}) \text{ s.t. } x \text{ は女性でない}$$

練習問題.

次の命題をを限定命題の記号を使って表現せよ。またその否定命題をつくれ。

この店の A セットを 30 分以内で食べた人は名前を貼り出してもらえる。

3 数の話

3.1 自然数

ものの個数を表すのに用いられる数

$$1, 2, 3, 4, 5, \dots$$

を自然数と言います. このような“数”に対する認識は (数を表記する方法が見つかるより) ずっと遠い昔からあったのは間違いないことですが, 現在ですら, 実際に私達が“自然”に出くわす自然数と言うのはそんなに種類があるわけではありません. (例えば 10,000,000,000,000,000 よりも大きな数字に出くわすことは普通にはまず無いでしょう.) このことを考えると上の 1, 2, 3, 4, 5, ... という表記の中の ... にはとても重要な意味があることが見て取れます.

寄り道 : 大きな数の表し方

上記の 10,000,000,000,000,000 は一兆の一万倍を表しており一京 (けい) と読みます. 日本語で大きな数を表すには次のような単位が用いられていました.

一 十 百 千 万 億 兆 京 (けい) 垓 (がい) し (禾へんに市, ただし文献によって異なる漢字を当てていることもあります) 穰 (じょう) 溝 (こう) 澗 (かん) 正 (せい) 載 (さい) 極 (きょく) 恒河沙 (こうがさ) 阿僧祇 (あそうぎ) 那由他 (なゆた) 不可思議 (ふかしぎ) 無量大数 (むりょうたいすう)

値としては, 万までは 10 倍ずつ, 万以上恒河沙までは万進, 恒河沙以上無量大数までは万万進となります.

ここでは現代数学では“自然数”をどのように定義しているのかを紹介します.(これは, あくまでも現代的な数学が「数」をどのように捉えているのか紹介しているだけです, 何を言っているのかよくわからなくてもあまり気にしないでください.)

ペアノの公理.

数の集まり \mathbf{N} があって次の 1 から 5 を満たしているとする.

1. $1 \in \mathbf{N}$ (1 と呼ばれる \mathbf{N} の元が一つ存在する.)
2. $\forall n \in \mathbf{N}, \exists n' \in \mathbf{N}$ (\mathbf{N} の任意の元 n に対して n' と書かれる \mathbf{N} が存在する. ... この n' のことを “ n の次の元” と呼ぶことにします.)
3. $\forall n \in \mathbf{N}, n' \neq 1$ (\mathbf{N} の任意の元 n に対して n' は 1 にはならない.)
4. $\forall n, m \in \mathbf{N}, n \neq m \rightarrow n' \neq m'$ (\mathbf{N} の任意の元 n, m に対して $n \neq m$ ならば $n' \neq m'$.)
5. $\forall M \subset \mathbf{N}$,

$$1 \in M \wedge (\forall n \in M, n' \in M \rightarrow M = \mathbf{N})$$

(\mathbf{N} の部分集合 M が “ $1 \in M$ ” かつ “任意の $n \in M$ に対して $n' \in M$ ” という性質を持つならば, M は \mathbf{N} に等しい.)

このとき \mathbf{N} を自然数の集合と言い、 \mathbf{N} の元を**自然数**と呼ぶ。

参考：

ジュゼッペ・ペアノ (Giuseppe Peano, 1858 年 8 月 27 日 ~ 1932 年 4 月 20 日) はイタリアの数学者。自然数の公理系 (ペアノの公理)、ペアノ曲線の考案者として知られる。

加法

加法 (足し算) をペアノの公理に基づいて考えることにしましょう。自然数 n に対して定まる次の元 n' を $n+1$ と書くことにします。 (つまり $n' = n+1$ と定めます。) そこでこの表記法を用いて $1' = 1+1$ を 2 , $2' = 2+1 = (1+1)+1$ を 3 , ... のように私達が慣れ親しんでいる表記法で表すことにします。

このような表記法に従って、任意の自然数 n に対して $(\dots(n+1)+1)\dots$ (m 個の 1 を足している) と表される自然数を $m+n$ と書き、 m と n の**和**と呼びます。つまり n から更に m だけ後ろにある数を $m+n$ と言うわけです。このようにして定まる加法に (+ の記号で定まる演算) に対して次のような性質が成り立つことを示すことができます。

$$\forall m, n \in \mathbf{N}, m+n = n+m$$

$$\forall l, m, n \in \mathbf{N}, (l+m)+n = l+(m+n)$$

(これは決して「あたりまえ」と言うことはできないことに注意してください。) 上に書かれた性質のうち最初のもの**交換法則**、二番目のものを**結合法則**と呼びます。これらは数学でより一般的な演算を取り扱うときに問題となる重要な性質です。

自然数の大小と減法

自然数の間の大小関係を次のように定めることにします：

二つの自然数 m, n に対して、 n にいくつかの数を加えて m が得られるとき、 m は n より**大きい**自然数であると言う。

そして m が n ときこれを

$$m > n$$

と表すことにします。

一般に m が n より大きいときある自然数 a が存在して $m+a = n$ が成り立ちますが、このような a を $m-n$ と表し、 m と n の**差**と呼ぶことにします。また m と n の差を求めることを**減法** (又は**引き算**) と呼ぶことにします。

つまり、標語的に言うと：

m と n の差を求める (このことを m から n を引くと表現することにします) とは,

n に足してやると m となるような数を求めること

となります.

乗法

自然数 m と n の乗法 (かけ算) と呼ばれる演算 \times を次のように定めます.

$$m \times n = m + m + \cdots + m \quad (m \text{ を } n \text{ 回足したもの})$$

またこの演算の結果得られた自然数 $m \times n$ のことを m と n の積と呼びます.

乗法の基本的な性質として交換法則と結合法則が成り立つということがあります. 即ち

$$\forall m, n \in \mathbf{N}, m \times n = n \times m$$

$$\forall l, m, n \in \mathbf{N}, l \times (m \times n) = (l \times m) \times n$$

が成り立ちます. (加法のときと同様にこれも「あたりまえ」ではなく, ちゃんとした証明をすべきことです.)

なお, かけ算の記号 \times は省略して書く (例えば $m \times n = mn$ のように書く) ことが良くあります.

分配法則

今までに出てきた自然数の“加法”と“乗法”の二つの演算に関して次のような性質が成り立つことも示せます.

$$\forall l, m, n \in \mathbf{N}, (l + m) \times n = l \times n + m \times n$$

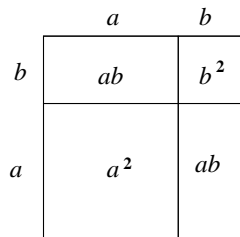
この性質を分配法則と呼びます.

3.2 分数

学問としての数学は今から 2400 年ほど前のギリシャで誕生しました。ギリシャ人は数を線分を用いて表していました。例えば $a + b$ は長さ a の線分と長さ b の線分をつなぎ合わせた線分で、また $a \times b$ は一辺が a 、他の一辺が b の長方形の面積として表すといった要領です。このような考え方をを用いると例えば次の図は公式

$$(a + b)^2 = a^2 + 2ab + b^2$$

を示していることとなります。



数を線分で表すという考えから、**分数**の概念は次のように出てきます。いま長さ 1 の線分の代わりに長さ 1 の糸を考えてやります。この糸を真ん中のところで半分に折るとこの糸の半分の長さが得られます。そこでこの長さを

$$\frac{1}{2}$$

と表してやることにします。同じように長さ 1 の糸を三つ折にして得られる長さを $\frac{1}{3}$ 、四つ折にして得られる長さを $\frac{1}{4}$ 、...、 m 等分になるように折って得られる長さを $\frac{1}{m}$ と表すことにします。

長さが $\frac{1}{2}$ の線分を二つつなげたものの長さを $\frac{2}{2}$ 、三つつなげたものの長さを $\frac{3}{2}$ 、四つつなげたものの長さを $\frac{4}{2}$ 、... のように書くことにします。このとき、 $\frac{1}{2}$ の線分を二つつなぐと 1 の長さ、四つつなぐと 2 の長さの線分になりますから

$$\frac{2}{2} = 1, \frac{4}{2} = 2, \dots$$

のような式が成り立ちます。

一般に、長さ $\frac{1}{m}$ の線分を次々とつないでゆくことにより

$$\frac{1}{m}, \frac{2}{m}, \frac{3}{m}, \dots, \frac{n}{m}, \dots$$

のような数が得られますがこのような数

$$\frac{n}{m}$$

を分数といいます。また m を**分母**、 n を**分子**といいます。

さて分数 $\frac{n}{m}$ は $\frac{1}{m}$ の長さの線分を n 個つないだ線分の長さを表しているわけですが、いまこの長さ $\frac{1}{m}$ の線分を更に等しい長さに k 回折り曲げた線分の長さを考えてみます。この線分を k 個つなげば長さ $\frac{1}{m}$ の線分になり更にこの線分を m 個つなげば長さが 1 の線分が得られます。従ってこの k 回折り曲げた線分を全体として mk 回つなげれば長さ 1 の線分が得られることとなります。従って次の式が成り立つことがわかりました。

$$\frac{n}{m} = \frac{nk}{mk}$$

この式を使うと例えば $\frac{48}{60} = \frac{4 \times 12}{5 \times 12} = \frac{4}{5}$ のように分数を簡単な形に書き直すことができます。このような操作を行うことを**約分する**と言います。

分数の足し算

$\frac{1}{3} + \frac{2}{5}$ のような長さを考えるにはどのようにすればよいでしょうか。この問題を考えるためには先ほど注意した式 $\frac{n}{m} = \frac{nk}{mk}$ が役に立ちます。

まずこの式により、 $\frac{1}{3} = \frac{1 \times 5}{3 \times 5} = \frac{5}{15}$ 、 $\frac{2}{5} = \frac{2 \times 3}{5 \times 3} = \frac{6}{15}$ となります。従って

$$\frac{1}{3} + \frac{2}{5} = \frac{5}{15} + \frac{6}{15} = \frac{11}{15}$$

と計算でき、求める長さは $\frac{11}{15}$ であることがわかります。

このようにいくつかの分数の分母を等しい数にそろえる操作のことを**通分**と言います。分母が違う二つの分数を通分するには機械的に二つの分母の積を新しい分母にすればうまくいきますが、例えば次のような例の場合には分母と分子にかける数をうまく工夫すれば計算はずっと楽になります。

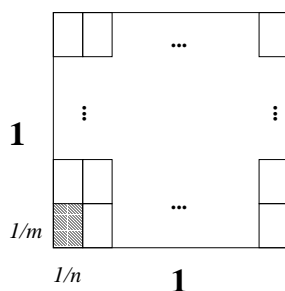
$$\frac{1}{15} + \frac{5}{6} = \frac{1 \times 2}{15 \times 2} + \frac{5 \times 5}{6 \times 5} = \frac{2 + 25}{30} = \frac{27}{30} = \frac{9}{10}$$

分数のかけ算

ここでは $\frac{1}{m} \times \frac{1}{n}$ のような計算を考えます。このためにまず、以前やった“かけ算は面積である”という考え方を思い出しておきます。二辺の長さがそれぞれ $\frac{1}{m}$ 、 $\frac{1}{n}$ の長方形の面積を考えます。このとき次の図からわかるようにこのような長方形は一辺の長さが 1 の正方形の中に mn 個入っています。

従って次の式が成り立つことがわかります。

$$\frac{1}{m} \times \frac{1}{n} = \frac{1}{mn}$$



次に $\frac{m'}{m} \times \frac{n'}{n}$ のような計算について考えます. これも上の図と同様の図を用いて考えると, 二辺の長さがそれぞれ $\frac{m'}{m}$, $\frac{n'}{n}$ の長方形の中には二辺の長さがそれぞれ $\frac{1}{m}$, $\frac{1}{n}$ の長方形が $m'n'$ 個入っています. 従って次の式が成り立つことがわかります.

$$\frac{m'}{m} \times \frac{n'}{n} = \frac{1}{mn} \times m'n' = \frac{m'n'}{mn}$$

つまり分数のかけ算は分母は分母, 分子は分子でかけ合わせればよい, ということになります.

自然数の割り算 (除法) と分数

まず自然数のかけ算

$$m \times n = m + m + \cdots + m \quad (m \text{ を } n \text{ 回足したもの})$$

を思い出しておきます. これは mn を作るには m を n 回足してやればよい, ということを言っている, と解釈できます. 例えば $16 = 2 \times 8$ は

16 の中に 2 が 8 個ある

ということも意味しています. そこでこのことを

$$16 \div 2 = 8$$

と表し, この演算 \div のことを**除法 (割り算)** と呼ぶことにします. より一般的な式で書くと

$$m \div n = a \Leftrightarrow m = na$$

ということになります.

さて自然数の引き算を説明したときに

m と n の差を求めるとは,

n に足してやると m となるような数を求めること

と説明しました。割り算を同様に標語的に述べると

m を n で割るとは

“ n にかけてやると m となる” ような数を求めること

ということができます。

さて二つの自然数の割り算は $9 \div 3 = 3$ のように自然数の中でできることもありますが、一般には $9 \div 4$ のように自然数の中に答えをみつけることができないこともあります。しかし答えとして分数を使ってもよいことにすると、自然数の割り算はいつでもできます。つぎにこのことを見ていきましょう。

例えば $2 \div 3$ のような割り算を考えて見ましょう。上で説明したよう、この割り算をするということは

“3 にかけてやると 2 となる” ような数を求めること

ということになります。分数のかけ算のところでやったように $3 \times \frac{2}{3} = \frac{3}{1} \times \frac{2}{3} = \frac{6}{3} = 2$ が成り立ちますから、この説明より $2 \div 3 = \frac{2}{3}$ となることがわかります。一般に $n \times \frac{m}{n}$ が成り立ちますから、これより次の式が成り立つことがわかります。

$$m \div n = \frac{m}{n}$$

分数の割り算

次に

$$\frac{m'}{n'} \div \frac{m}{n}$$

のような分数の割り算について考えます。ここでちょっと天下りの的ですが $\frac{m'n}{n'm}$ という数を考えることにし、この数に $\frac{m}{n}$ かけてみます。すると

$$\frac{m'n}{n'm} \times \frac{m}{n} = \dots = \frac{m'nm}{n'mn} = \dots = \frac{m'}{n'}$$

となりますが、これは

$$\frac{m'}{n'} \div \frac{m}{n} = \frac{m'n}{n'm}$$

ということの意味しています。このように書くと意味がわかりにくいですが言い換えると

分数で割り算をするには分母と分子を取り替えてかけ算をすればよい

ということができます。

3.3 負の数, 整数, 有理数

数字を個数を数えるためであるとか, 長さを測るためのものという認識をしている限り 0 という数字を考える必然性はあまりありません(「個数が 0」であるとか「長さが 0」ということは要するに「何も無い」ということですから, 何も考える必要は無い訳です). しかし例えば山の高さを測ってそれを数字を使って記録するために海面の高さを 0m と定めこれを基準にすることにしました. この基準を用いると, 海面下の位置の“高さ”はマイナス何 m といった言い回しで表すことができます. つまり海面の高さから 100m 下にあるところは“マイナス 100m”の位置にある, という具合です. 更に高さ 200m の山から 300m 下るとマイナス 100m の地点に到達する, といった“計算”もできます. このように位置を測るための物差しとしての考え方をすれば, 負の数とその加法, 減法が自然に導入されるでしょう. ここではそのことを見てゆくことにしましょう.

0 の導入

自然数が拡張されて 0 という数字が導入されるまでには数学の歴史では非常に長い時間がかかりました.(「何も無いことをあらわす数字」と言うものを生み出すには数字に対する考えのレベルが大きく飛躍する必要があったことは, 容易に想像できるでしょう.) 0(零)はインドで発見されましたが, それがいつごろであるか, まただれがなし遂げた仕事であるかは知られていません. インドの最初の天文学者アリアバタ(5世紀)は零を知っていたらと推定されています. 今日使用している零の確かな記録は, 876年, インドで書かれたものがあるそうです.

現代数学では 0 次のように定義されます.

0 とは任意の数 x に対して

$$x + 0 = 0 + x = x$$

となるような数である.(ここでは「数」が何を意味するのかは気にしないことにします.)

この定義を用いると次のようなことがわかります.

0 は一つだけしか存在しない

また分配法則を用いると次がわかります.

任意の数 x に対して $0 \times x = 0$

負の数

この節の始めに述べたように負の数を表すために，“物差し”を導入することにします．ここでは普通の物差しではなく，左右に無限に伸びる直線上に，基準になる点 0 をとって，その右に等間隔に $1, 2, 3, \dots$ と目盛りをつけ，左にも順に等間隔に $-1, -2, -3, \dots$ と目盛りをつけます．

...

引き算は「幾何学的」な言葉で考え表現することができます．例えば「 N から 2 引く」という操作は，

数直線上で 2 分左にずらす

と理解することができます．これは「引き算は足し算の逆の操作」という考えと完全に適合する捕え方になっていることに注意してください．また「 N に -2 を足す」という操作も

数直線上で 2 分左にずらす

と表現できますから，この事と「引き算は足し算の逆の操作」という“原理”を合わせてやると「 N から -2 引く」という操作は

数直線上で 2 分右にずらす

に対応することがわかります．すなわち

$$N - (-2) \text{ は } N + 2 \text{ に等しい}$$

ことがわかります．

自然数 $1, 2, 3, \dots$ に 0 と $-1, -2, -3, \dots$ を加えた数の全体を総称して**整数**と言います．なお整数の全体からなる集合は普通、太字の \mathbf{Z} または \mathbb{Z} で表しますが，これはドイツ語 Zahlen (数・複数形) からきたものです．

整数 a, b (ただし b は 0 でない) を用いて $\frac{a}{b}$ と (分数で) 表せる数を**有理数**と言います．有理数全体の集合は，記号 \mathbf{Q} または \mathbb{Q} で表します．

まとめ

負の数は数直線の上で表現するのが自然である．またそこでの正 (負) の数の足し算，引き算は数直線上で点を右や左 (左や右) にずらす操作と考えるとよい．

必然なのか、定義なのか？(なぜ「負の数かける負の数は正」になるのか)

例えば中学で習った

$$(-1) \times (-5) = 5$$

という式は「正しい」のでしょうか？またもし「正しい」のなら、ここで言う「正しい」とはいったいどう意味なのでしょう？

ここではこの問いに対して少し説明を試みてみます。まず歴史的には負の数は「負債(借金)」を象徴したものである(「九章算術」紀元1世紀, 中国)と言うことを思い出しておいてください。例えば誰かから5ドル借りたらその人は自分の台帳に -5 と書きます。3人の人から5ドルずつ借りたときは台帳には

$$3 \times (-5) = -15$$

と書くこととなります。一般に N 人から5ドルずつ借りた場合この人の借金は

$$N \times (-5)$$

となります。ところでこの人がもし一人の人に借金を返したら借金をしている人は一人減って $N-1$ 人となります。この時のやり取りは

$$(*) \quad N \times (-5) + 5 = (N-1) \times (-5)$$

と書くのは自然でしょう。

さてここで上の式は N が0の時にも成り立つとします。すなわち上の式(*)は

$$0 \times (-5) + 5 = (0-1) \times (-5)$$

となります。 $0 \times (-5)$ というのは借金がいない状態を意味しますからこれは0です。したがって左辺は $0 \times (-5) + 5 = 5$ となります。一方右辺は $(0-1) \times (-5) = (-1) \times (-5)$ という形になっています。したがって、

$$5 = (-1) \times (-5)$$

が分かりました。

…しかしこの計算は正しいと言えるのでしょうか？この計算は $N=0$ の時にも式(*)が成り立つことを前提にしたものですが、このような前提が許される根拠は一体どこにあるのでしょうか？

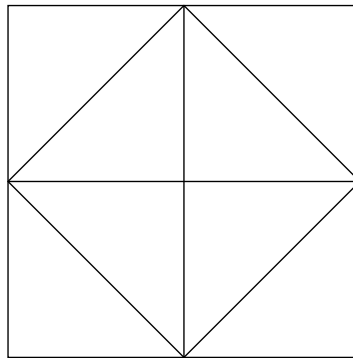
この問題については、後で「複素数」について学ぶときにまた取り扱うことにします。

3.4 無理数

ある数 x に対して、2乗(：自乗)すると x になるような数のことを x の**平方根**といいます。例えば 4はその(正の)平方根として2をもちます。

正の数 x に対してその正の数の平方根を \sqrt{x} とかくことにします。さて幾何学では平方根は線の長さとしてよく出てきます。まずその一例を紹介しましょう。

ある日ソクラテスは若い奴隷にある正方形の2倍の面積をもつ正方形を作るように言いました。次の図はソクラテスはそのヒントとして書いたものです。



いま、もとの正方形の面積は1であるとしします。このとき新しく得られた正方形の一辺の長さは $\sqrt{2}$ になるというわけです。(なお、16世紀のイタリアでは平方根のことを単に lato(辺)と呼んでいました。)

寄り道：ギリシアの三大作図問題

上の問題と類似した次の問題は「三大作図問題」と呼ばれギリシア時代から長い間数学者を悩ませ続けましたが、結局19世紀にこれらの問題は定規とコンパスによる作図では解けないことが証明されました。

1. 与えられた円と等しい面積をもつ正方形を作ること(円積問題)
2. 与えられた立方体の体積の2倍に等しい体積をもつ立方体を作ること(立方体倍積問題)
3. 与えられた角を三等分すること(角の三等分問題)

上のようにして得られる数 $\sqrt{2}$ が分数では表せないということをピタゴラス学派の人たちは知っていました。ここでは $\sqrt{2}$ が分数で表せないことの証明を紹介しましょう。

はじめに $\sqrt{2}$ が分数で表せると仮定します。つまりある自然数 A, B が存在して

$$\sqrt{2} = \frac{A}{B}$$

とかけたと仮定します。必要ならこの分数を約分し新しく得られた分数を考えることにより、この分数 $\frac{A}{B}$ はもうこれ以上約分できないと仮定しても良いでしょう。従って特に A と B 両方が偶数であることはありません。

ステップ 1 $\sqrt{2}$ の定義を利用する

上の式を 2 乗することにより次の式が得られます。

$$(\sqrt{2})^2 = \left(\frac{A}{B}\right)^2$$

この式は次のように変形できます。

$$2 = \frac{A^2}{B^2}$$

ステップ 2 A が偶数であることを示す

上の式 $2 = \frac{A^2}{B^2}$ の両辺に B^2 をかけると次の式が得られます。

$$2B^2 = A^2$$

これから A^2 は偶数であることがわかります。ところでいま

どんな奇数も 2 乗するとまた奇数になる

(残念ながら、この講義ではこのことは証明しません)

ことが知られているので、これから A は偶数であることがわかります。

ステップ 3 B が偶数であることを示す

ステップ 2 で A が偶数であることがわかりましたので、ある自然数 C が存在して $A = 2C$ と書けます。そこでこの式の両辺を 2 乗すると

$$A^2 = 4C^2$$

これとステップ 2 の式 $2B^2 = A^2$ より、

$$2B^2 = 4C^2$$

が得られます。この式の両辺を 2 で割ると

$$B^2 = 2C^2$$

が得られますが、これに ステップ 2 の時と同じ議論を適用してやることにより B が偶数であることがわかります。

最終ステップ 矛盾点を見つける

ステップ 2 と 3 で示したこと (A も B も偶数になる) ははじめにのところで確認した仮定「A と B 両方が偶数であることはない」に矛盾します. よってこれより, $\sqrt{2}$ は分数で表せないことがわかりました.

3.5 実数の小数表示

有理数は分数によって表されました. では $\sqrt{2}$ のような無理数はどのように表せるのでしょうか? ここでは $\sqrt{2}$ を小数を使って表す方法について紹介しましょう.

まず, $1 < \sqrt{2} < 2$ となることを示します. いま $1 \geq \sqrt{2}$ とします. この式の両辺に $\sqrt{2}$ をかけることにより, $\sqrt{2} \geq 2$ が得られますが, この式と最初に仮定した $1 \geq \sqrt{2}$ より $1 \geq 2$ が得られますがこれは明らかに矛盾です. 従って $1 < \sqrt{2}$ となることがわかりました. 同様に $\sqrt{2} < 2$ となることもわかります.

さて同様に $1.4 < \sqrt{2} < 1.5$ (即ち $\frac{14}{10} < \sqrt{2} < \frac{15}{10}$) となることが示せます. 実際, $1.4 \geq \sqrt{2}$ と仮定してみます. $1.4 \geq \sqrt{2}$ の両辺に 1.4 をかけてやると, $(1.4)^2 (= 1.96) \geq 1.4\sqrt{2}$ が得られます. また $1.4 \geq \sqrt{2}$ の両辺に $\sqrt{2}$ をかけてやると, $1.4\sqrt{2} \geq 2$ が得られます. これら二つの式を合わせてやると $1.96 \geq 2$ となることがわかりますがこれは矛盾です. 同様に $\sqrt{2} < 1.5$ となることもわかります.

以下同様に繰り返してゆくと $1.41 < \sqrt{2} < 1.42$, $1.414 < \sqrt{2} < 1.415, \dots$ という具合に $\sqrt{2}$ の表示をいくらでも先まで求めることができます.

デデキントの切断.

$\sqrt{2}$ は上のようにしていくらでも有限の桁数を持つ小数 (これは必ず小数で表せます) を使ってその上と下から “近似” してゆけることがわかりました. ドイツの数学者 デデキント (1831-1916) はこのような考え方を発展させて有理数の切断 (Schnitt) という考え方を導入し **実数** を定義しました. ここではデデキントの考え方を簡単に紹介しましょう.

有理数の全体を次の条件を満たすような二つの組 A, B に分けます.

1. A, B はともに空ではない.
2. A に属する有理数は常に B に属する有理数より小さい.

このとき, A, B の組 (A, B) のことを**切断**と呼びます. 切断 (A, B) に対しては次のいずれかが成り立ちます.

- I. A には最大の有理数があるが, B には最小の有理数がない.
- II. A には最大の有理数がないが, B には最小の有理数がある.
- III. A には最大の有理数がなく, B には最小の有理数がない.

デデキントは切断 (A, B) を**実数**と呼び, I 又は II でのような実数を **有理数**, III のような実数を **無理数** と名づけました.

カントールの集合論

無理数を取り扱うにあたっては「無限」を避けて通ることはできません。「無限」について初めて取り組んだ数学者がカントール (Georg Cantor : 1845-1918) です。彼の理論“集合論”は 20 世紀数学の原理化体系化抽象化公理化などにも大きな役割を果たしています。

カントールは 1845 年 3 月 3 日ロシアのペテルスブルグ (レニングラード) にゲオルグ・ボルデマーとマリアの長男として生まれました。お父さんはユダヤ系の商人で、一家は 1856 年にドイツに移住します。1866 年 21 歳のカントールはベルリン大学を卒業しベルリンで当時最高の数学者のもとで研究することになりました。1878 年には 1 対 1 の対応から集合の“大きさ”を表す濃度の概念を得て、まず有理数の全体及び代数的な数の全体が自然数全体の濃度と同じである (可付番) ことを証明しています。

濃度

例えば、自然数全体と偶数全体の間には

自然数	1	2	3	4	5	6	7	8	...	n	...
	↓	↓	↓	↓	↓	↓	↓	↓		↓	
偶数	2	4	6	8	10	12	14	16	...	2n	...

と対応を余りなくつけることができます。このようなとき「自然数全体と偶数全体の濃度は等しい」と言います。

更にカントールは実数の濃度が可付番より大きいことを証明しました。カントールの集合論は革命的であったため当時の多くの数学者から受け入れられず疑問をもたれていました。特に彼の師クロネッカーは数学全体を自然数の直観にもとづいて厳密に構成すべきだという強い信念を持っていたので、その意味で厳密に定義のできない集合概念には反対でした。彼はカントールのことを“いかさま科学者”“裏切り者”，“若者を墮落させる男”などと呼びさまざまな嫌がらせをしました。

当時の集合論への反対に対して、カントールは次のように書いています。

数学はその発展のためには絶対的に自由でありただ 1 つの必要条件はその概念が内部矛盾を含まないということだけである。

彼はその後「連続体仮説」(“可付番と実数の間の濃度は存在するか”という問題)に熱中しますがなかなか解答が得られず加えてクロネッカーが自分の論文を発表させないようにするのはないかという心配が重なり、1884 年に最初の break down(精神異常)をおこしました。その後も彼はこの病から回復することはなく、死ぬまで入退院を繰り返すことになります。この「連続体仮説」から来るストレスが、病気の発作の引き金になっていたようです。

結局彼はこの解決を見ることはありませんでしたが、この問題は 1950 年代後半にアメリカの若き数学者コーエン (Paul Joseph Cohen, 1934 年 -) によって意外な形で解決されることになります。

4 複素数

4.1 方程式の歴史

未知の量を求めるときそれがわかっているような振りをしてそれが満たすべき式 (方程式) を立てて、その式を解いてやることにより答えが得られることがよくあります。現在私たちが知っている方程式のは 17 世紀のフランソワ・ヴィエテの著作「解析技術入門」の中で初めて現れましたが、このような数の取り扱い方については実ははるか昔にすでに知られていました。

ここでは「解析技術入門」以前のエジプト、バビロニアでどのような問題が取り扱われていたのか紹介することにします。

リンド・パピルス

紀元前 1700 年ごろのエジプトのパピルス (古代の紙) の中には次のような問題とその解答が記されていました。

問題 1. ある数と、その $\frac{1}{7}$ とを合わせると 19 になる。ある数を求めよ。

解. ある数を 7 と仮定せよ。7 のひとつとその $\frac{1}{7}$ で 8 となる。19 を得るためには、8 は何倍かせねばならない。そのかけるべき数 ($\frac{19}{8}$ のことです) を 7 にかけると求める答え ($:\frac{133}{8}$) を得る。

(解説) ある数を x とするとこの問題は方程式 $\frac{8}{7}x = 19$ を考えることになります。これを解くと $x = 7 \times \frac{19}{8}$ となりますが、上の解はこれを求めていることにほかなりません。

バビロニアの数学

チグリス・ユーフラテス河流域のバビロニアでもエジプトと同時期に高度の文化をもった社会が展開しました。バビロニアでは記録を粘土板に残していましたが、これによって紀元前 2000 年頃には次のような問題取り扱われていたことがわかっています。

問題 2. 長さ x と幅 y がある。分母は長さで、その逆数は幅である。長さの 12 倍は深さ z である。その体積は 20 である。この長さ x と幅 y と深さ z は何ほどか。

解. 12 の逆数を求め、それを 20 倍すると $\frac{20}{12} = \frac{5}{3}$ をえる。これが長さである。この逆数 $\frac{3}{5}$ が幅で 20 は深さである。

(解説) 長さ、幅、深さをそれぞれ x, y, z とすると与えられた問題は

$$\begin{cases} y = \frac{1}{x} \\ 12x = z \\ xyz = 20 \end{cases}$$

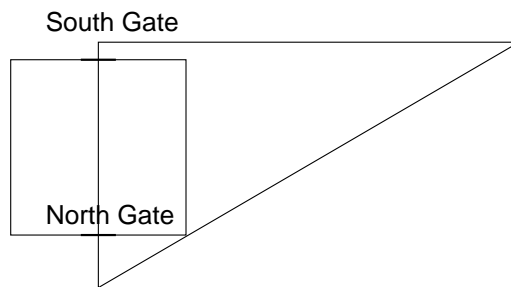
となります。一番目の式を三番目の式に代入すると $z = 20$ を得ます。これを 2 番目の式に代入して $12x = 20$ となります。これを解いたのが上の解の最初の答えになっています。

エジプトやバビロニアにおいては方程式の一般的な解き方については記載されておらずそこでは上のような具体的な問題だけが取り扱われていました。なおバビロニアでは 2 次方程式なども考察されており、実質的には 2 次方程式の解の公式なども知られていたようです。

また中国の九章算術(紀元 1 世紀)の中には次のような問題があります。

問題 3. 正方形の邑(むら：大きな村のこと)がある。その大小はわからない。各辺のちょうど中央に門がある。北門を出てちょうど 20 歩の所に木がある。南門を出て 14 歩折れて西に 1775 歩行って木を見ることができた。邑の方(：一辺の長さのこと)は何程か。

(解説) 邑の一辺の長さを x とすると次の図と相似な三角形の二辺の長さの比が等しいことから $\frac{x}{2} : 20 = 1775 : (x + 34)$ を得ます。この式から 2 次方程式 $x^2 + 34x = 71000$ を得ますのでこれを解けば良いわけです。ただ中国では方程式の一般解を求めるといった理論は現れず、このような方程式が与えられたときにその近似解を求めるにはどうしたらよいか? という方向に発展して行ったようです。



寄り道：代数学

代数学は数学の一分野で、「代数」の名の通り数の代わりに文字を用いて方程式の解法を研究する学問として始まりました。ただし現代では、代数学はその範囲を大きく広げているため、「数の代わりに文字を用いる数学」とか「方程式の解法の学問」とかいう理解の仕方は適当ではありません。

このような代数学が生まれた背景には、インド・アラビア数字(算用数字)とその計算法の普及があります。算用数字 1,2,3,4,5,6,7,8,9 の起源は古代インド(紀元前)とされているますが、零 0 と位取り記数法が初めて登場した時期は 6~7 世紀頃ではないかと考えられています。イラン東部に 749 年に始まるアッバース朝はバグダッドに首都をおき、産業・文化の水準を高めました。イスラム帝国は、アジア・アフリカ・ヨーロッパの 3 大陸にまたがり、しかも当時の世界の中心に位置していたため、イラン・ギリシア・ローマ・中国・インドなどの優れた先進文化を受け継ぎ、アラビア語を共通言語としてそれを統合発展させました。9 世紀には、アル・スワーリズミーが「インド記数法」を著し算用数字を用いた計算を紹介しています。この本は、12 世紀前半にラテン語に訳され、インド・アラビア数字がヨーロッパに知られる元になりました。当時ヨーロッパではローマ帝国以降、ローマ数字が用いられ、計算は計算玉を用いる計算板が利用されていました。算用数字は

筆算の計算を可能にすることから、大変有用でこれを紹介した書籍としてピサのレオナルド (: フィボナッチ) による算術書 (1205) などが出版されました。

なおアル・スワーズミーは「復元と対比の整理」という本も著していますが、この原題中の「アル・ジャブル (al-jabr)」という言葉 (移項を意味する) が、代数学を意味する「アルジェブラ (algebra)」の語源となっています。

4.2 複素数

2 次方程式 $ax^2 + bx + c = 0$ の解の公式

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

は実質的には古代バビロニアで知られていたようです。ここで $b^2 - 4ac < 0$ となるような方程式では $\sqrt{\quad}$ のなか負の数になってしまいますが、16 世紀の頃まではこのような数 (複素数) を考えることはありませんでした。従って、このような方程式は考える必要がないと考えていられたようです。ところが 16 世紀にイタリアの数学者タルタリア (N. Tartaglia, 1499–1567) によって 3 次方程式の解の公式が発見されると奇妙なことに、最終的に実数の解が得られるような方程式でも、公式にあてはめて計算する過程では複素数が現れることがありました。つまり計算の途中で複素数を利用してさまざまな計算をする必要があるというわけです。しかしこのような複素数が積極的に認められるようになるには、まだしばらくの時間が必要でした。この節では、複素数をその計算について紹介し、さらにその図形的なイメージについて述べてみたいと思います。

複素数の計算

いま i を $i^2 = -1$ をみたす “数” とし

$$a + ib \quad (a, b \text{ は実数})$$

の形で表される数のことを**複素数**とよびます。また i のことを**虚数単位**、 $b \neq 0$ のとき $a + ib$ を**虚数**、 $a = 0$ のとき ib のことを**純虚数**とよびます。

複素数 $a + ib$, $c + id$ の和、差は次のように計算されます。

$$(a + ib) \pm (c + id) = (a \pm c) + i(b \pm d)$$

また積 (かけ算) は、($i^2 = -1$ に注意すると) 次のようになることがわかります。

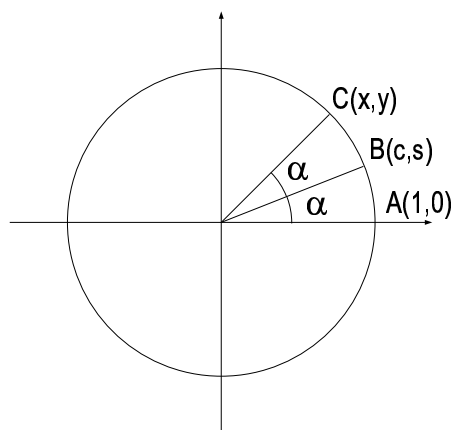
$$(a + ib)(c + id) = a(c + id) + ib(c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc)$$

由来の違う同じ形の式

フランスの数学者アブラハム・ド・モアブル (Abraham de Moivre, 1667 年 5 月 26 日 - 1754 年 11 月 27 日) は 1707 年に円弧を n 等分するという幾何学的な問題と、 n 乗してやると与えられた複素

数になる複素数を求める (与えられた複素数の n 乗根を求める) という問題の類似性に気づきました. ここで, 簡単にド・モアブルの結果について紹介しましょう.

まず xy 平面内の半径 1 の円周を考えこの図の中で三点 A, B, C を次の図のように定めます.



このとき三角関数の 2 倍角の公式

$$\cos 2\alpha = \cos^2 \alpha - \sin^2 \alpha, \quad \sin 2\alpha = 2 \sin \alpha \cos \alpha$$

により, 点 C の座標 (x, y) は, 点 B の座標 (c, s) を使って

$$x = c^2 - s^2, \quad y = 2cs$$

と表せることが分かります. ド・モアブルは, 複素数 $c + is$ を 2 乗するとこの式が出てくることに気がつきました. つまり

$$(c + is)^2 = (c^2 - s^2) + i(2cs)$$

書き換えると

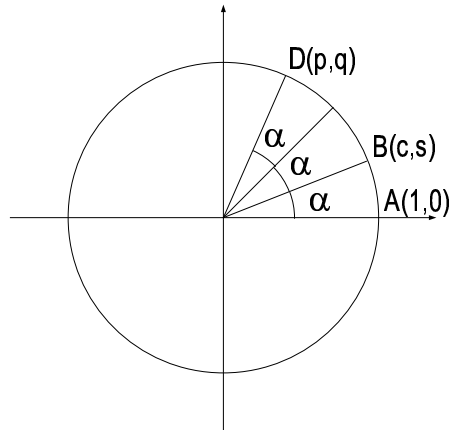
$$(c + is)^2 = x + iy$$

となるのです. さらに三角関数の 3 倍角の公式を使うと図のような三点 A, B, D に対して

$$(c + is)^3 = p + iq$$

が成り立つことが示せます.

ド・モアブルはこのような観察を続け今日「ド・モアブルの公式」と呼ばれる次の公式を発見するに至りました.

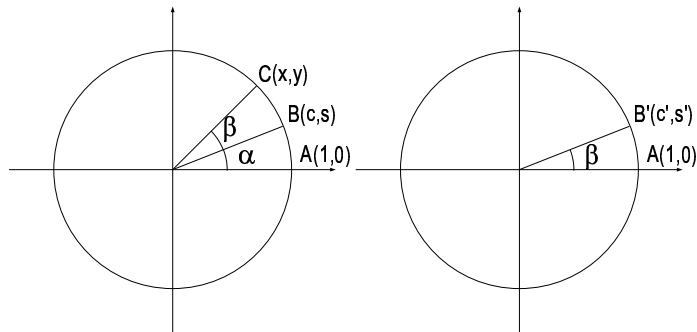


$$(\cos \alpha + i \sin \alpha)^n = (\cos n\alpha + i \sin n\alpha)$$

またド・モアブルの仕事ではありませんがこれと類似の例として三角関数の加法公式

$$\sin(\alpha + \beta) = \sin \alpha \cos \beta + \sin \beta \cos \alpha, \quad \cos(\alpha + \beta) = \cos \alpha \cos \beta - \sin \alpha \sin \beta$$

について考えてみましょう。これに対して次のような図を考えてやります。



この式から今度は

$$x = cc' - ss', \quad y = sc' + s'c$$

という関係式が読み取れます。一方2つの複素数 $c + is$ と $c' + is'$ をとってやると

$$(c + is)(c' + is') = (cc' - ss') + i(sc' + s'c)$$

という式になりまたも同じ式が出てきました。このような三角関数と複素数との類似はどのように解釈すべきなのでしょう、あるいはどのように解釈してやるのが最も自然なのでしょう。

複素平面

1797年にノルウェーの数学者カスパー・ヴェッセル (Casper Wessel) によって、複素数の幾何学的な解釈 (複素平面) が与えられました。残念ながら彼の仕事はその後 100 年ほど歴史の中に埋もれてしまいましたが、1832年数学の王者と呼ばれているガウス (Karl Friedrich Gauss, 1777~1855, ドイツ) はこの結果を再発見し複素数を基礎付ける理論を完成しました。(複素平面のことをガウス平面と呼ぶことも良くあります。) ここでは複素平面の考え方について紹介します。

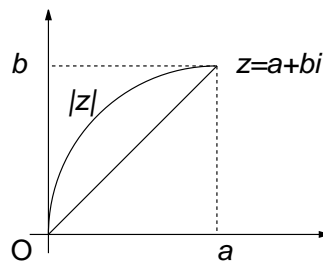
複素数 $z = a + bi$ に対して、座標平面 (xy 平面) 上の点 (a, b) を考えると、複素数とこの平面上の点は 1 対 1 に対応します。このように複素数に座標平面の点を対応させるとき、この座標平面を**複素平面**と呼びます。

・複素数の絶対値

複素平面上の点 z と原点 O との間の距離を複素数 z の**絶対値**といい $|z|$ で表します。即ち $z = a + bi$ に対して

$$|z| = |a + bi| = \sqrt{a^2 + b^2}$$

となります。

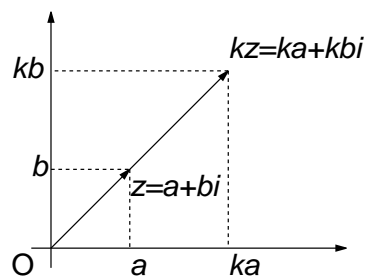


・複素数の正の実数倍

複素数 $z = a + bi$ と実数 k の積は、

$$kz = ka + kbi$$

となりますから、複素平面上では次のように表されます。つまり複素平面全体では原点を中心に平面全体を k 倍に拡大縮小することに対応しています。



・複素数の極形式

複素平面上で、0でない複素数 $z = a + bi$ を表す点を P とかくことにします。このとき次の図のように OP の長さ ($|z|$ のことです) を r , OP が x 軸となす角を θ とすると

$$a = r \cos \theta, \quad b = r \sin \theta$$

とかけること、よって

$$z = r(\cos \theta + i \sin \theta)$$

となることがわかります。このような z の表示のことを複素数 z の**極形式**と呼びます。

この極形式を使って複素数の積を計算してみましょう。2つの複素数 z, w を極形式を使って

$$z = r(\cos \alpha + i \sin \alpha), \quad w = s(\cos \beta + i \sin \beta)$$

このとき上で述べたように加法定理がうまく使えて zw が次のように計算できます。

$$\begin{aligned} zw &= r(\cos \alpha + i \sin \alpha) \times s(\cos \beta + i \sin \beta) \\ &= rs(\cos \alpha + i \sin \alpha)(\cos \beta + i \sin \beta) = rs(\cos(\alpha + \beta) + i \sin(\alpha + \beta)) \end{aligned}$$

これから複素数 zw は複素平面上で原点からの距離が rs , また x 軸となす角度が $\alpha + \beta$ であるような点に対応することが分かります。つまり「複素数 z に複素数 w をかける」とは「複素平面上で z に対応する点を、まず原点からの距離を s 倍に拡大してそれから原点の周りを角度 β だけ回転させ」た結果得られた点に対応させる、とすることができます。

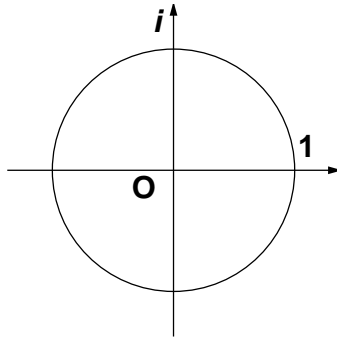
例. 上で述べたような幾何学的な解釈を使って \sqrt{i} を計算してみましょう。いま

$$\sqrt{i} = r(\cos \alpha + i \sin \alpha)$$

とすると、この両辺を2乗して

$$i = r^2(\cos 2\alpha + i \sin 2\alpha)$$

を得ます。ここで $i = 0 + i \times 1 = \cos(\pi/2) + i \sin(\pi/2)$ ですからこれから $r = 1$ (r は原点からの距離なので $r > 0$ となることに注意してください) と $2\alpha = \pi/2$ を得ます。このとき α としては $\pi/4$ と $5\pi/4$ の2つの可能性があることに注意してください。従って $\sqrt{i} = \cos(\pi/4) + i \sin(\pi/4) = 1/\sqrt{2} + i/\sqrt{2}$ または $\sqrt{i} = \cos(5\pi/4) + i \sin(5\pi/4) = -1/\sqrt{2} - i/\sqrt{2}$ を得ます。



・ $(-1) \times (-1) = ?$

さて上で述べた複素平面の考え方をを用いて $(-1) \times (-1)$ の計算をして見ましょう。

$$-1 = -1 + i \times 0 = \cos \pi + i \sin \pi$$

ですから「 -1 をかける」という操作は、複素平面上の点を原点の周りに 180 度回転させることに
 対応することが分かります。このことより $(-1) \times (-1) = 1$ となることが分かります。また同様に
 して $(-2) \times (-3) = 6$ など、つまり「負の数に負の数をかけると正になる」ことが従います。

5 暗号

5.1 古典的暗号

暗号 (cryptography) とは一般的に「情報の交換や記憶集積に関して、第三者にそれが知られることや、あるいは当事者をも含めて故意による情報の改変を防ぐために、その対象となる情報を秘匿するための技術や方法のこと」と定義されます。このように情報を秘匿して伝える方法に関しては紀元前5世紀のギリシアですでに書字版の木の部分に文字を記録しその上から蠟を厚く塗って文字を隠す、というやり方で無事メッセージを届けたことが知られています。このように普通の文章を隠すタイプの秘密通信は、厳密には、暗号ではなく「ステガノグラフィー」と呼ばれますが、このような方法では、もしその情報が見つければその通信の内容がすぐに明らかになるという欠点があります。暗号は情報の存在を隠すのではなく、その内容を隠すことをその目的としています。この内容を隠すプロセスのことを**暗号化**、また暗号化された情報から元の情報を再現することを**復号化**と呼びます。暗号化、復号化を行なうためには発信者と受信者があらかじめ決めておいた暗号の規約(=プロトコル)にしたがってメッセージを暗号化、復号化します。このようなプロトコルの例としては次のようなものがあります。

シフト暗号 [shift cipher]

紀元前1世紀のローマの軍事的指導者であるジュリアス・シーザーによって用いられた最も古典的な暗号方式です。カエサル暗号、シーザー暗号と呼ばれることもあります。具体的には平文の文字をそれぞれ鍵で与えられた文字数分だけずらすことによってメッセージを暗号化します。例えば(3文字ずらす場合)

this is a pen → wklv lv d shq

となります。しかし、この暗号は文字の種類の数(英語なら26, 日本語なら50)しか存在しないので全ての鍵を試せば簡単に破ることができます。

換字暗号 [substitution cipher]

換字暗号とは、文字を何かに置き換えることにより暗号文とする暗号化方式で、暗号文は文字である必要はありません。シャーロックホームズのシリーズに『踊る人形』と言う作品がありますが、これは、アルファベットを人形の踊っている姿で置き換えたものです。このような暗号は7世紀から全盛期を迎えたイスラム世界で国家機密などを安全に伝えるために用いられました。

具体的な例で説明します。以下の文を暗号化(Encrypt)することを考えます。

THIS IS A PEN

いま以下の表にしたがって文字を置き換える事によって暗号化を行なうことにします。

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	S	N	I	U	B	Z	K	X	M	W	O	T	C	E	V	Y	Q	F	A	H	L	J	P	G	D

すなわち、TをFに置き換え、HをZに置き換え…、といった様に文中の文字を置き換えていきます。その結果結果は以下のような文字列 (暗号文) が得られます。

F Z K Q D K Q D R D E I T

以下では、暗号化前の文を平文 (Plain Text または Clear Text)、暗号化後の文を暗号文 (Cipher Text) と呼ぶことにします。文字の置き換えを逆に辿れば暗号文を元の平文に戻すことができます。

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 S N I U B Z K X M W O T C E V Y Q F A H L J P G D

このように暗号文から平文を得る事を復号化 (Decrypt) と呼ぶことにします。二者間で文書を暗号化して送るには、あらかじめ

“ R S N I U B Z K X M W O T C E V Y Q F A H L J P G D ”

という文字列を二者間で合意しておく必要があります。悪意ある第三者 (Tamper) に対してこの文字列をもらしさえしなければ、通信経路が盗聴される可能性があったとしても、安全 (Secure) な情報交換を行なう事ができる。このように、暗号化・復号化を行なうために必要な情報は鍵 (Key) と呼ばれます。上記例では、“ R S N I U B Z K X M W O T C E V Y Q F A H L J P G D ” という文字列が鍵になります。このように暗号化するための鍵と復号化する為の鍵が同じであるような暗号方式のことを、**対称暗号方式**と呼びます。対称暗号方式における鍵は、場面によって対称鍵 (Symmetric Key)、共通鍵・共有鍵 (Session Key)、秘密鍵 (Secret Key) などと呼ばれます。

換字暗号は暗号化するための方法の数はシフト暗号よりも多く安全性は高いといえますが、文字の頻度を変える事ができないので、十分な長さの暗号文があれば破ることができます。実際、アラビア人たちはこのような暗号を解読するための方法についても研究していましたが彼らが用いた方法は**頻度分析**と呼ばれる方法です。例えば、換字暗号で暗号化された英語の文章があったとします。まずその文章の中の各文字の出現頻度を数えます。最もよく現れる文字が分かればそれを英語の文章の中でもっとも出現頻度の高い e と置き換えます。次に頻出する文字を次に出現頻度の高い t または a に置き換えます。このような操作を繰り返して、暫定的に暗号化された文章の各文字にアルファベットを割り当ててやります。普通はこれではちゃんとした文章にはなりません、英語の特性 (例えば冠詞は a, an, the となる) を考えながら、この暫定的なアルファベットの割り当てを修正してやる事により、暗号を解読することが出来ます。

例.

vyq nkvnq tcddkv, c yjkgv tcddkv, cpf c dncem tcddkv, nkxgf kp c nctig hqtguv.

gxgta oqtpkpi vjga jqrrgf qvw qh dgf cpf qvw kpvq vjg gctna oqtpkpi uwpujkpg.

vjga nxkgf vq urgpf cnn fca rncakpi vqigvjgt.

暗号化のための方法を秘密にしておくのは非常に困難ですが、鍵はいろいろ変更することができます。そこで暗号の安全性はその鍵の秘密を守れるかによっていると考えべきです。1883年「軍用暗号」のなかでアウグスト・ケルクホフス・フォン・ニーウエンホフは

「暗号システムの安全性は、暗号化アルゴリズムを秘密に出来るかには関係せず、鍵の秘密が守られるかどうかにかかっている。」

と述べましたが、これは現在に至るまで暗号理論の基礎に横たわる原理です。

ヴィジュネル暗号, エニグマ

上記のように換字式暗号は頻度分析を用いて解読することが可能です。このような欠点を補うより強力な暗号がヴィジュネル (フランス, 1523年生まれ) によって考案されました (ヴィジュネル暗号)。これは 鍵 で定められたやり方に応じてシーザー暗号での文字のずらし方を次々と切り替えてゆくというもので、十分に長い鍵を使い、更にメッセージを送るたびに鍵を変えてやれば解読することは不可能です。

```
a: 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
b: 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
c: 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
d: 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
e: 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
f: 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
g: 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
.
.
.
z: 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
```

例えば, this is a pen を age という 鍵 を用いて暗号化するには次のようにします。

```
this is a pen   →   t h i s i s a p e n
      鍵                a g e a g e a g e a
暗号化された文章   t n m s o w a v i n
```

このような操作を自動化するものとして第2次世界大戦中にドイツ軍が用いた「エニグマ」と呼ばれる装置があります。(ただしこのエニグマもその内部構造の特殊性などを利用して解読することが可能でした。)

対称暗号方式では鍵が第三者に知られた時点でその暗号は無効化されるため、共通鍵の共有が常に問題となります。一般的にはこの共有のためには大変な実際上労力が必要となります (鍵配送問題)。

5.2 鍵配送問題

(暗号について考えるときには, アリス (A), ボブ (B), イヴ (E) という三人が登場し, アリスがボブに, そしてボブがアリスにメッセージを送ろうとしイヴがそれを盗聴しようとする, という

例え話をすることが多いのでここでもそれに従うことにします.)

クイズ 1.

いまアリスとボブは郵便局員のモラルが非常に低い国に住んでいる（この国の郵便局員イヴは鍵（南京錠）のかかった箱に入っていない手紙はすべて盗み見てしまう）とします。アリスもボブもそれぞれ自分の南京錠とその鍵は持っているのですが、お互いに相手の南京錠の鍵は持っていないとします。このような状況で郵便だけを用いてイヴにその内容を見られることなくメッセージをやり取りするにはどうすればよいでしょうか？

クイズ 2.

いまアリスとボブはほかの人に知られること無くひとつの色のペンキを共有する必要があるとする（この色は何色でも良い）とします。但しアリスからボブ、ボブからアリスに送るペンキの色はすべてイヴには分かってしまうとします。このような状況の下でイヴに知られること無くアリスとボブが共通の色を持つためにはどうすればよいでしょうか？

（ヒント：二つの色ペンキを混ぜてできるペンキの色が分かったとしても元の二つの色は分からない。特に元の二色のうちのひとつが分かってももうひとつの色が何であるか知ることは難しいとします。）

このクイズ 2 における色の役目をするものとして**モジュラー演算 (時計算)**と呼ばれるものがあります。以下これを用いて上のクイズ 2 に当たる操作をどのように実行するのかについて紹介します。

定義. m を自然数とする。整数 a と b に対して、 $a - b$ が m で割り切れるとき、 a と b は m を法として合同であるといい、 $a \equiv b \pmod{m}$ とかく。

例えば 7 を法とした世界では足し算はようになります。このような計算をモジュラー演算と呼びます。

$$2 + 3 \equiv 5 \pmod{7}$$

$$2 + 4 \equiv 6 \pmod{7}$$

$$2 + 5 \equiv 0 \pmod{7}$$

$$2 + 6 \equiv 1 \pmod{7}$$

$$2 + 7 \equiv 2 \pmod{7}$$

またモジュラー演算の世界では次のようにして指数関数を考えることもできます。

$$3^2 \equiv 9 \equiv 2 \pmod{7}$$

$$3^3 \equiv 27 \equiv 6 \pmod{7}$$

$$3^4 \equiv 81 \equiv 4 \pmod{7}$$

$$3^5 \equiv 243 \equiv 5 \pmod{7}$$

$$3^6 \equiv 729 \equiv 1 \pmod{7}$$

ところで一般に m が十分に大きいとき与えられた整数 y, t に対して $y^x \equiv t \pmod{m}$ という x の方程式を解くことは非常に難しいことが知られています。そこで $y, x \rightarrow y^x$ を y と x という「色」を混ぜる操作と考えるとすることにより以下のようにして鍵の交換を行えることがわかります。

モジュラー演算を利用した鍵交換

アリスとボブはすでに $y^x \equiv t \pmod{m}$ の式において $y = 7, m = 11$ ととることに合意している。(このことはイヴに知られていてもかまわない.)

STEP1.

アリス

アリスは数 A を一つ選び (例えば 3 を選んだとします) それを秘密にしておきます。

アリスは $7^A \equiv 7^3 \equiv 343 \equiv 2 \pmod{11}$ を計算します。この計算結果 (: 2) を α と呼ぶことにしこれをボブに伝えます。

ボブ

ボブは数 B を一つ選び (例えば 6 を選んだとします) それを秘密にしておきます。

ボブは $7^B \equiv 7^6 \equiv 117649 \equiv 4 \pmod{11}$ を計算します。この計算結果 (: 4) を β と呼ぶことにしこれをボブに伝えます。

STEP2.

アリスとボブが連絡を取り合う過程でこの α, β がイヴに知られてしまうかもしれませんがそれはかまいません。

STEP3.

アリス

アリスはボブの結果 β を使って β^A を計算します。 $4^3 \equiv 64 \equiv 9 \pmod{11}$

ボブ

ボブはアリスの結果 α を使って α^B を計算します. $2^6 \equiv 64 \equiv 9 \pmod{11}$

STEP4.

このようにしてアリスとボブはイブに知られることなく同じ数字 9 を得ることができました. この 9 を暗号の鍵として用いてやることができます.

以上のような鍵交換方法のアイデアは 1976 年にディフィー・ヘルマン・マークルの三人の暗号学者によって発表され暗号の研究者たちを驚嘆させましたが, 実用化の上ではまだ次のような問題点がありました.

1. 実際にメッセージのやり取りをする前に鍵のやり取りをする必要があります. この点は例えば電子メールなどでメッセージをやり取りする上で, いつでもメッセージを送れる, というその利点を減じてしまいます.
2. この方法だと他人がアリスになりすましてボブにメッセージを送ったとしてもボブにはそのことを確かめることができません.

5.3 公開鍵暗号

ここまで紹介してきた暗号は全て暗号化と復号化に同じ鍵を用いてきました (対称鍵). ディフィー前の節の最後に述べた問題点を克服するためには暗号化と復号化に別の鍵を用いる暗号システム (非対称鍵の暗号システム) という考え方を考案しました. もしこのような暗号システムが実際にあれば, アリスは暗号化の鍵を自分専用にもっておいて復号化の鍵を公開することによって, 十分実用的な暗号を使うことができるようになります (公開鍵暗号). ただディフィーはこのようなアイデアを提案しましたが, これをどのようにして実現するのかその方法まで与えることはできませんでした.

RSA

非対称鍵というアイデアを実現しようと多くの研究者が努力をしましたが 1977 年リヴェスト・シャミア・アドルマンの三人の研究者はこれに成功し今日 **RSA** と呼ばれ広く用いられている暗号システムを提出しました.

ここではこの暗号システムについてごくごく簡単に説明しましょう.

p, q を非常に大きな (201桁程度) の二つの異なる公表されていない素数とします. このとき次のような自然数や自然数の集合を用意します.

$$N = pq \quad (\text{この } p \text{ と } q \text{ は非公開とします})$$

$$L = (p-1)(q-1)$$

ℓ : $p-1$ と $q-1$ の最小公倍数

$$M = \{ 400 \text{桁以下の自然数で } N \text{ と互いに素なもの} \}$$

このとき『公開鍵』 $\{c, N\}$ と『秘密鍵』 d を次のように定めます.

c : L と互いに素な ℓ 以下の自然数.

d : $cd \equiv 1 \pmod{L}$ となる ℓ 以下の自然数. (このような d はユークリッドの互除法と呼ばれる方法を用いて求めることができます.)

このとき M の元を次のように暗号化します :

$$m \rightarrow m^c \pmod{N}$$

このようにして得られた暗号は次のようにしてやれば元の数に戻ることが知られています.

$$m \rightarrow m^d \pmod{N}$$

いまもとのデータ M を復号化するためには 2 つの素数 p と q を知る必要があります. $N = pq$ は公開されているのでこれから p, q を求めるのは簡単に思えますが N が 400 桁くらいの数字になると, 実際に N を因数分解して p, q を求めるのはほとんど不可能といわれています. したがって RSA は安全であるといえるわけです.

ところで RSA は次のような特性を持っています.

「秘密鍵を用いて暗号化した文書は公開鍵を用いて復号化できる」

この性質を用いると例えばアリスがボブに文書を送るときに自分の秘密鍵を用いて暗号化してしてやればボブはアリスの公開鍵を用いてこれを復号化することができるわけです. このときアリスの秘密鍵はアリスしか持っていないわけですから, ボブはこの文書は確かにアリスから送られたものであることを確認できます (デジタル署名).

このような利点があり RSA は現在インターネット上でもっとも広く使われている暗号となっていますが, 現在も多くの数学者や暗号研究者によって様々な新しい暗号が提案されています.