はしがき

あえて「イマイチ」

なぜ「イマイチ」かと言われると困ってしまうが、とにかく今、数学で自分の立ち位置がヘンだと思っている諸君を何とかしよう という講座である．

次に聞かれるのは「レベルは？」ということだが、これも関係ない．私はそういう「切り口」で生徒を見たことがない．しかし、**やる気**だけは持ってきてもらいたい．

何がヘンなのかがわかればもうヘンではないのだ．こまごまとしたことはここには書かない．受けてもらえば自然にわかると思う．

この冊子の意味

街の本屋の棚を見てもらいたい．こう言ってははばかるが、問題集はヤマのようにあっても、**基本原理**をキッチリと書いた参考書らしいものはほとんど見かけない．そして受験生は問題集のことを参考書だと思っているらしい．

それに、困ったことに諸君は、問題をたくさん解いて練習すれば実力がつくと思っているようだ．しかし、それはちょっと当たっているが大きくまちがっている．

そこで、私としては自前で「それらしいモノ」を書くことにした．このテキストは私がパソコンを打ち、河合塾のスタッフに作ってもらったいわば**手作り**の**特注品**である．

実際、60 歳を過ぎてのパソコンは少々キツかった．夜中まで血圧を気にしながら人差し指でキーボードをつつく爺さんを想像できるか———正気の沙汰ではない．

まあ、それやこれやでとにかくできた．君たちがつかまっても沈没しない**「べた書き筏(いかだ)」**は、ほぼ完成した．これには安心してしがみついてよい．

ここでハッキリ言っておくが、易しいことは易しいし、難しいことはやはり難しい．これは仕方がない．まして数学が君に擦り寄ってくることなどあろうはずがない．

だから、どうしても超えなければならないヤマならば、君が出かけて行って君の実力で乗り越えるほかはないのである．ここにはそのための道具がすべてつまっている．

筆者としては、大学に進もうとする若者が知っているべき最小限のことがらを、その将来を見据えて、なるべく順序だてて**「べた書き」**にした．

若者には無限の可能性がある

この歳になって振り返ってみると「人生は意外に短いなあ」とつくづく思う．私にも君の年齢があった．何もわからずウロウロと極楽トンボをやっていたのであろう．

生きるということは次々に可能性を剥奪されることなのです．まず、やりたいことを決めなさい．そして、それに向かって全力で頑張れ．道は君の後にできるものだ．

ハラを括るのは今、先に延ばせばそれだけ困難になる．爺さんになったから言えることだが、君たち若者が本気になってやれないことなどあるわけがない．

才能？、そんなものはやっているうちに出てくるよ．何でもやってみなければわかるものか．自分では何も気がついていないだろうが、君の人生はまだ始まってもいない．すべては今から始まるのです．

2015 年 04 月 17 日　　諸橋　実

＜追記＞

数学ってナンダ

まあ、いろいろな立場からいろいろな考え方があろうが、私はここで数学はキレイだとか、数学はすばらしい、などというつもりはサラサラない．しかし、とりあえず

数学とは**数と量**に関する**言語**である

ということは誰もが素朴に認める共通認識としてもよかろう．まず、ここからはじめよう．

その上でこの科目をサボルとどうなるか．結果、数と量に関する認識があいまいになり、それにかかわるコミニュケーションが破綻する———これは世界の半分を失うことではないか．

何も専門家になれというのではない．しかし、そのことから人々の「判断の信頼性」が失墜し、社会そのものの崩壊にもつながるハナシなのだ．だから本来、どうしてもこの科目を避けて通ることはできない．そういうことなら、いっそハラを据えて徹底的にやればよいではないか．

ヤルなら効率よく

私は「問題演習をドンドンやればデキルようになる」という信仰を否定するつもりはない．確かにそういう一面もある．しかし、去年の問題も、一昨年の問題も解いて、····· のようなことをしていたのでは「来年出るはずの問題」も練習をしなければならなくなるのではないか．

しかし、この科目はタダの暗記科目ではない．数学はその個々の概念が、「関係」として**体系的に構成されている**という特殊な性質がある．だから、何年の何大学の問題である、というような切り口からではその問題の核心に届かない———その問題の、数学としての根っこを捕まえてザックリやるしかない．たとえば確率の例でいうと、素人 (生徒) サンは

さいころの問題、くじ引きに問題、袋から球を出す問題、·····

のように、みんなちがうハナシに見えてしまう．しかし、数学としての立場はちがう．つまり

数学的確率の定義、加法定理、条件つき確率、乗法定理、·····

と数学の体系に沿って考える．要するに「さいころの問題」と「くじ引きの問題」は素材がちがっても、数学的確率という同じ体系のカケラなのだ．それは、去年の問題も一昨年の問題も、はたまた来年出る問題も、東大の問題も早稲田の問題も、結局は同じマナイタで調理さたモノなのである．そういうことなら、こちらとしても個々の知識をバラバラに覚えるのではいかにも非効率である．だったら、その体系ごとゴッソリとさらってしまえばよいではないか．

公式について

あるとき教室で「自分で証明できない公式は使うな！」と言ってみたのだが、そのときの反応がおもしろかった．どうやら、そういうことは考えてみたこともないらしいのである．

大体、自分で確かめてもいないことを振り回す根性も気に入らないが、それより、そういうことではその公式が正しく使えているとは思えない．公式というのは、それぞれの数理現象をとりまとめて数式などで簡潔に表したものだからうまく使えば便利なものではある．しかし、その背景を正しく把握していないと十分に使いこなせない．そういうものなのである．

つまり公式は、先に述べた「数学の体系」で言えば骨に当たるものであろう．しかし、タダの骨だけでは何の役にも立たない．君の手でその証明を確認し、その意味を探り、時には感動もし、そういうことを通して君にとって血の通った道具にしなければ意味はない．実際、使い物にもならない．それでこそ、その有難さもわかってくるというものだ．ラクをした分のツケは大きいぞ．

別人になろう

まず、「知る」と言うことはどういうことか．あるとき授業の後で、「今、言ったことを全て忘れてもらって、全くなかったことにしよう」と言ったら、「それはできない」と言う．

そうです．知るということはそういうことなのです．つまり、知る前の君と知ってからの君とは全くの**別人**なのです．一旦知ってしまったことを忘れてもとの君にはもどれない．

「知る」ことにより、そして**「考える」**ことにより、人は強くなる．生涯、人は強くなり続けるしかない．だから、君の闘う相手は他人ではなくて君自身であり、良くも悪しくも君のいま立っている所がつねに君の出発点なのです．それが生きることの基本原理なのだと私は思います．

2015 年 10 月 03 日　　著者記す

目 次

第 1 章　基礎編 **5**
1.1　序論———整数とは何か 6
1.1.1　自然数 6
1.1.1.1　自然数の定義 6
1.1.1.2　日常感覚と数学 8
1.1.1.3　「 数の概念 」の拡張 11
1.1.2　p 進法 28
1.1.2.1　p 進法による n 桁の表示 31
1.1.2.2　p 進法表示で表された数を q 進法表示になおす 32
1.2　整数入門———整除の定理 39
1.2.1　約数・倍数 42
1.2.1.1　整除の可能性と一意性 42
1.2.1.2　約数、倍数の定義 44
1.2.2　最大公約数・最小公倍数 46
1.2.2.1　定義 46
1.2.2.2　「 最大公約数 」、「 最小公倍数 」に関する定理 47
1.2.2.3　ユークリッドの互除法 54
1.2.3　剰余類 61
1.2.3.1　剰余系と類別 61
1.2.3.2　合同式 68
1.3　素数と素因数分解、他 82
1.3.1　素数と合成数 82
1.3.1.1　素数 82
1.3.1.2　素因数分解 88
1.4　整数論的関数 90
1.4.1　約数の個数とその総和 91
1.4.2　オイラーの関数 95
1.4.3　ガウスの関数 98

第 2 章　応用編 **109**
2.1　方程式の整数解、他 110
2.1.1　1 次の不定方程式 111
2.1.1.1　$ax + by = c$ 111
2.1.1.2　$ax + by + cz = d$ 123
2.1.2　2 次の不定方程式 126

2.1.2.1 $axy + bx + cy + d = 0$ 127
2.1.2.2 判別式の利用 129
2.1.2.3 いろいろな方程式 133
2.1.3 不等式の整数解 136
2.2 その他についての発展的考察 139
2.2.1 ペル方程式 139
2.2.1.1 解集合の構造 139
2.2.1.2 整数解を求める 142

第1章　基礎編

神は整数をつくり給うた．のこりはすべて人間の業である．

レオポルド・クロネッカー

この言葉に筆者は少なからず衝撃を受けた．長い長い時間をかけて**数の概念**を日常から切り離し、**有理数**、そして**無理数**、さらに**虚数**へと数の概念を拡張し、数学という抽象された数理現象の世界を体系化した、人間という生き物の不思議を思わないではいられない．そして、その抽象の世界で構成された体系が、具体的な現実の世界をシッカリと支えているということが、さらに大きな不思議である．

そして、今日、私たちは、好むと好まざるとにかかわらず、しかも当たり前のようにその中にドップリ浸かって、享受すべきは享受し、何の疑問も持たずに生きている．

この稿を書きながらつくづく思ったが、これは**奇跡**であって、とても当たり前のことではない．何と名づければ胸に落ちる表現ができるのか．

何ともウマイ言葉が見当たらないが、それは、長い苦闘の末、人間が自然から切り取った**自由**とでもいうものであろうか．その歴史はまさに**大河ドラマ**ともいうことができるであろう．

まあ、文章で書けばこういうことで、何となくロマンチックではあるが、概ねの諸君からは「そんなことよりどこがでるの？」と聞かれそうではある．

実際、この章の内容から入試問題の素材が選ばれることも多いが、そういうことより整数という分野全体の基礎知識を歴史的な話題をもつつきながら、より明確に整理することを目的にしている と考えてもらえばよい．

しかし、こうして書いてみて改めて筆者の感想を言えば「やはり整数は難しい」というのが実感である．それは、パターン化してチャンチャンとは行かない．その都度ごとに自分のアタマで考えることをせめられるからであろう．

だから、あわてなくてよろしい．君だけが難しいわけではない．できる限りメリハリをつけて整理して書いたから、１つ１つをシッカリ読み込んでもらえば「大満足」とは行かないかもしれないが「ソコソコ満足」という程度にはわかってもらえると思う．

そういうこともあって、本来はこのあとに続くべき**不定方程式**は章を改めて解説することにした．やはり、これがよさそうな気がする．

1.1　序論———整数とは何か

1.1.1　自然数

1.1.1.1　自然数の定義

3 人の子ども (この集合を A とする) がいて、3 つのりんご (この集合を B とする) があるとき、この 3 人の子どもにこれらのりんごを 1 つずつ分配すれば過不足がない.

つまり、2 つの集合 $A,\ B$ の間に **1 対 1 の対応**がつけられる．このとき、2 つの集合 A と B は**同じ大きさ**であるといい、その**大きさが 3 である**という.

ここで注目すべきは、3 人の子どもや 3 つのりんごは目に見えるが、3 という数は目に見えない．このように、具体的ないろいろな事物の集合から、他の一切の特徴を排除して、**1 対 1 に対応する**という点にのみ注目して、その共通性を抽象したものが**自然数**である.

しかし、自然数にはもう 1 つの面がある．それは、第 1 番目、第 2 番目、$\cdots\cdots$ のように順序を表す場合である.

自然数を、個数を表すために用いる場合、これを**基数**、または**計量数**といい、順序を表すために用いた場合、これを**序数**、または**順序数**といい、自然数がこのような二面性をもつことを最初に指摘しておこう.

数の概念が最初に発生したのは、おそらくは基数としてであろう．しかし、数が基数として成立する以前に、量として多いか少ないかの関係にしたがった順序づけがあるはずだから、それは同時に序数でもあったはずである.

まあ、基数が先か序数が先かについては、いろいろ議論のあるところだが、いずれにしても、数が数として成立するには、まずそれが**質から区別された量**でなければならないことは確かである.

数学の理論では、この自然数のもつ二面性をいちいち区別せずに、ただ「 **数** 」として統一的に考えている．そして、数がもっとも威力を発揮するのは、具体的な数量とか順序とかにいちいち拘束されないで、**形式的に「 計算できる 」**というこの 1 点においてであろう.

ところで、この $1,\ 2,\ 3,\ 4,\ \cdots\cdots\cdots$ という**自然数**には、次のような性質があることをわれわれは知っている——-以下、数字はすべて自然数を表すものとする.

(1) 自然数は 1 から始まり、次々に進んで行くと得られる数である.

(2) 物を数えるときに使われる.

(3) 大小の順序がある———任意の自然数 $a,\ b$ については、$a > b,\ a = b,\ a < b$ のうち、1 つだけが成り立つ.

(4) $a,\ b$ を加えることができる．そして、その結果は一意的に確定する.

(5) $a > b$ なら a から b を引くことができる.

(6) a と b はいつでも「 カケル 」ことができる.

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

まだ他にもいろいろな性質を挙げることができるだろうが、このような性質を踏まえた上で、**自然数を定義する**ことを考えるのである.

その方法としては、まず、このような様々な性質のうち、ある性質があればそこから他の性質が導き出されるような**最も基本的な性質**を見つける———**公理**を定める.

そして、それを出発点にしてそこから導き出されるものを次々に証明しながら**理論体系を構成する**、というのが数学の立場である.

とはいえ、所詮は目に見えないものから出発し、目に見えないまま構成された理論体系を、モノのありようとしての日常に、何の矛盾もなく、アタリマエのこととしてそのまま有効に反映させている人間という生き物の**その能力**というか、あるいは**その実態**に、改めて驚嘆せざるを得ない.

ともあれ、何千年もの間、晒され、敲かれ、削られ、磨かれて今日に至る、人々の知恵の集積のようなものである———先人の英知を借りることにしよう.

イタリアの数学者**ペアノ (1858〜1932)** は、彼の論文「 数の概念について 」(1891) に、次の 5 つを「 原始命題 」(公理のこと！) としてあげ、それから数の理論を展開することを試みている———21 世紀のわれわれとしても、確かなカタチで数を議論するにはここまでさかのぼらなければならない.

それは、**1，後続，自然数** の 3 つを**無定義概念** (無条件に認める概念) として，次の (1)〜(5) を**自然数の公理**とした———**ペアノの公理**といわれている.

すなわち

(1) 1 は自然数である.
(2) 任意の自然数 x に対して，その後続 x' となる自然数 x' が 1 つだけある.
(3) $x' = y'$ ならば $x = y$ である.
(4) $x' = 1$ となる自然数 x は存在しない.
(5) 1 がある性質をもち，その性質をもつ自然数 x の後続 x' が，またその性質をもつとすれば，すべての自然数がその性質をもつ.

これは、**序数**の面からみて、その基本的な性質を抽象したものであるが、これだけの公理から、自然数に関する他のいろいろな概念が定義され、われわれが経験的に知っているいろいろな性質が導かれる のである.

特に (5) は**数学的帰納法の公理**といわれ、自然数だけでなく、広く数学の論証に重要な役割を果たしている.

何やら難しそうなことをゴタゴタと書いてきたが、要するに「 **自然数とは何か** 」と問われれば、上記の **(1)〜(5) を満たす集合 $\boldsymbol{N}$** のことである、と理解しておけばよい. ともかく、このようにして人々は**数の概念**を獲得してきたのである.

(注) 数の抽象性

「 数の世界 」には「 3 人の子ども 」とか「 3 つのりんご 」とか、そういう具体性は一切ない. そういうものをすべて捨象した「 計算だけの世界 」である. ここでは、こういう世界を獲得し、構築してきた**人間**という生き物の**不思議**を、ちょっとだけ考えてもらえば十分である.

(注) ＜ end ＞

1.1.1.2　日常感覚と数学

自然数は、私たちが物心のつくか、つかないかの幼いころ、とにかく、生まれて初めて出会った数である．そして以来、ずっと付き合ってきた．

今となると、これを「 数 」として意識したのがいつのことであったかさえ、もはや定かでない．それは、あまりにも**当たり前**のこととして来たし、実際に日常の世界に身をおく限り、当たり前以上でも以下でもないから仕方がないのである．

しかし、それを**整数論**という数学の方法論の中で**認識**するとなるとハナシは全くちがってくる———ここのところがヤッカイなのだ．

先に述べたように、数学は**公理**から出発し、そこから導かれる様々な事実からその**理論体系**を構成するのが身上である．そうなると日常の感覚での「 当たり前 」もその完璧な理論体系の前には、そのままの当たり前ではすまないことが起こる．

そういう事情で、私たちが慣れ親しんで十分ワカッテイルはずの、この「 **整数** 」というテーマを学ぶについても、その日常的な理解の１つ１つを「 数学の身上 」に照らして、「 許されるかどうか 」を**検証**する必要が生じてくる———ここが何とも悩ましい．

おそらく世に「 数学嫌い 」が生ずる原因の１つはこの辺にあるのかも知れないが、さりとて数学が微笑んで擦り寄ってくる、などということは絶対にありえない．

そういうことなら、いっそ数学の個性を尊重して「 言い分の１つも聞いてやろう 」ではないか———まあ、大体はそこから始まるのです．

以下、数学が日常の「 当たり前 」をどう表現するかの例を２つほど挙げておく．あまり難しく考えず、サラリと読んでもらいたい．

定理

自然数の集合は、それが空集合でない限り、最小数が存在する．

(**解説**) 何ということはない——**あったりまえ**のことではないか．と、一応はそう思う．

しかし、実はそう当たり前のことでもないのである．上記では、ハナから**自然数の集合**となっている——だから「 当たり前 」と思ったのだ．

しかし、これが整数の集合となるとハナシはちがってくる．つまり

$$\{\cdots\cdots\cdots\cdots, -2, -1,\ 0,\ 1,\ 2,\ \cdots\cdots\cdots\cdots\}$$

には**最小数がない**——負の数でどこまでも小さい数が存在する．

また、有理数の集合 $\{x|\ 1 < x < 2\}$ では、x はどこまでも 1 に近い有理数値をとることができるが、1 そのものになることはない．だから、**最小値はない**．

もう 1 つ挙げておこう．

$$\left\{\frac{1}{\sqrt{2}},\ \left(\frac{1}{\sqrt{2}}\right)^2,\ \left(\frac{1}{\sqrt{2}}\right)^3,\ \left(\frac{1}{\sqrt{2}}\right)^4,\ \cdots\cdots\cdots\cdots\cdots\cdots\right\}$$

は、どこまでも 0 に近い値が出てくるが、0 となることはなく、**最小値はない**．このように見てくるとこの定理は、**自然数の集合**を他の集合と区別し、特徴づける重要な性質の 1 つを述べていることがわかるだろう．

しかし、その証明となると、そう簡単ではない——大体、「 当たり前のこと 」の証明は難しい場合が多いようである．

この定理もキチンと証明しておきたいが、先を急ぐのでここでは触れない．ただ、どこかで出会うこともあろうから、証明には「 前掲の **ペアノの公理 (5)** を使う 」とだけ付け足しておく——この公理と同値なのだ．

さて、この定理を**整数** (0 および、負の整数を含む) の場合にまで**一般化**すると次のようになる．すなわち

> 整数 (自然数、0、負の整数) の集合を S とすると、S のすべての要素が、ある整数 k よりも小さくない (これを**下に有界**という) ならば S には最小数がある．

となる．上記の定理は、この表現の $k = 1$ の特別の場合であると考えればよい．なお、S が**上に有界**の場合は最大数がある．

＜ end. ＞

アルキメデスの原理

任意の整数 $a,\ b\ (a>0)$ に対して、 $b<na$ を満たす自然数 n が存在する．

(**解説**) これも当たり前である．$a>0$ だから、a で割って与えられた不等式を変形すれば、もっとよくわかる．すなわち

$$\frac{b}{a}<n \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

を満たす自然数 n があるというのだが、$b \leqq 0$ ならば $n=1$ でも 2 でも、自然数なら何でもよい．

また $b>0$ ならば、$\dfrac{b}{a}$ は正の数だから、自然数 n はいくらでも大きくとることができるので、$(*)$ を満たすような n が存在することは当たり前である．

しかし、**数学の方法論**は、常識的、経験的にいかに明らかに見えることであっても、それが**公理系から演繹的に導ける**ことを確かめながら、一歩一歩前進していく、という方法をとるのである．

この**アルキメデスの原理**は、これを日常的、即物的にいえば、たとえば $b>0$ の場合でいうと、ロールに巻いた長い長い布があったとして、これを長さ a の物差しで測るとしよう．このとき、$(n-1)$ 個分がとれて、n 個とると b を越えてしまうような、そういう n が存在する、ということで、どんな大きな b であっても、a (それがどんな大きな自然数であっても) でいつかは測りきれる、というほどの意味である．

そんなことはアタリマエのことではないか——やってみるまでもなく、想像するだけでわかる．しかし、この原理を**数学の身上**にしたがって証明すると次のようなことになる．

(証明) a は自然数だから

$$a \geqq 1 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

(i) $b>0$ のとき： b より大きい n をとれば

$$n>b \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ②$$

n は正だから、① の両辺に n をかけると

$$na \geqq n \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ③$$

②, ③ より $na>b$ が成り立つ．

(ii) $b \leqq 0$ のとき： $a>0$ だから

$$a>b \qquad \therefore\ a\cdot 1>b$$

で、$n=1$ にとればよい．

以上により、b の正、負、0 に関係なく $na>b$ となる自然数 n が存在することが証明された．

＜ end. ＞

1.1.1.3 「 数の概念 」の拡張

自然数の「 **加法** 」は、**基数**の立場からは、集合の大きさ、すなわち、和集合の大きさととらえることができる．たとえば、 $3+2=5$ は、計量数 3 の集合と、これとは別の計量数 2 の集合の和集合の計量数が 5 であるということである——2 つの自然数の組 $(3,\ 2)$ が 1 つの自然数 5 に対応していると見ることができる．

一方、**序数**の立場から見ると、3 の次の次の数が 5 ということである——これも、2 つの自然数の組 $(3,\ 2)$ が 1 つの自然数 5 に対応している対応関係である．

そして、いずれの場合も、2 つの自然数の組 $(3,\ 2)$ が 1 つの自然数 5 に対応する対応関係である——1 つの自然数が指定されて確定する．

つまり、自然数の**加法**とは、自然数の**順序対** (つい) である $\boldsymbol{(a,\ b)}$ を自然数 $\boldsymbol{a+b}$ に対応させる 1 つの**写像** (対応関係) である と見ることができる．

同様にして、自然数の「 **乗法** 」も、自然数の**順序対**である $\boldsymbol{(a,\ b)}$ を自然数 $\boldsymbol{ab}$ に対応させるもう 1 つの**写像**である．

ちなみに、**順序対**とは、「 順序を指定して定めたもの 」という意味である．そして、$a,\ b,\ c$ が自然数の集合 N の要素であるとき、これらについては、一般に次の性質が成り立つ．すなわち

(1) $\boldsymbol{a+(b+c)=(a+b)+c}$ (**和の結合則**)
(2) $\boldsymbol{a+b=b+a}$ (**和の交換則**)
(3) $\boldsymbol{a(bc)=(ab)c}$ (**積の結合則**)
(4) $\boldsymbol{ab=ba}$ (**積の交換則**)
(5) $\boldsymbol{a(b+c)=ab+ac}$ (**第 1 分配則**), $\boldsymbol{(a+b)c=ac+bc}$ (**第 2 分配則**)

だが、これらの法則は、帰納的に導かれるだけではなく、正確に証明することができる．

それは、前掲の**ペアノの公理**から演繹するのであるが、ここでは、これ以上深くは立ち入らない．機会を作って、自分でつなげておいてもらいたい．

さて、かくして自然数 N の集合では

$$\boldsymbol{a\in N,\ b\in N}\ \textbf{ならば、}\boldsymbol{a+b\in N,\ ab\in N}\cdots\cdots\cdots\cdots\cdots(*)$$

が成り立ち、このとき、自然数 N の集合は**加法**、**乗法**について「 **閉じている** 」という．まあ、ここまでは誰もが認めるだろう．しかし、この先がヤッカイだ．

つまり、数学としては、**加法**、**乗法**、そしてその**逆演算**として定義される**減法**、**除法**のすべて (これを**四則演算**という) を目指したいわけである．

以下、自然数の限界を確認しながら、「 **0** や**負の整数** 」を含んだ新しい数の概念として**整数全体**の集合への拡張、そして**有理数** (分数で表される数) の集合への拡張について、簡単に説明する——おおよそのキブンがわかってもらえればよいと思う．

＜1＞「 0 」と「 負の整数 」を含む「 整数全体 」への拡張

そこで、**減法**とは何か――それは、加法の**逆演算**として定義される．たとえば、**減法「 $\boldsymbol{b-a}$ 」**とは

$$\boldsymbol{x+a=b} \longleftarrow \text{「 } a \text{ に何を足したら } b \text{ になるか 」ということ！}$$

を満たすような x を見出すことである．しかし、$b=5$ で $a=3$ なら $x=2$ は明らかだが、$b=3$ で $a=5$ のようなときは、上記を満たす自然数 x は存在しない．

こういうとき、**減法**という「 **新しい演算** 」に対して自然数の集合 N は**閉じていない**という――自然数 N の集合だけではこの演算をまかなえない．

しかし、数学としては、この**減法**という新しい演算に対しても、自然数という**制約**にとらわれることなく、**自由に**この演算を遂行したい．そのためには、この演算についても**閉じている**ような「 **新しい数の集合** 」を、新たに作り出さなければならないという事情が起こってきたのである．

ここで読者は、大きく深呼吸を、いや、ちょっと外の空気を吸って気分転換をしてきてもらいたい――ここからが本番なのだ．

さて、**減法**という新しい演算を遂行するために数学は何をしたか．まず、「 2 つの**自然数**の**順序対**である $(\boldsymbol{a},\ \boldsymbol{b})$ で定まる $\boldsymbol{a-b}$ のすべて 」を「 **新しい数** 」と考えることにした――まだ「 0 」や「 負の数 」が普及する以前の状態だと思ってもらいたい．

つまり、自然数とその演算である加法しか持ち合わせていない．この状態で、こうして得られた数の間に、自然数の場合に成り立つ**関係**に合わせて

等しい，　加法，　減法，　乗法

などという**関係**が、「 そのまま成り立つように 」決めるのである．と言ってもピンとこないだろうから、具体的にそれらをすべて書き上げてみると

$\boldsymbol{a>b}$ **のとき**は

$$\left.\begin{array}{l} 2-1=4-3=5-4=\cdots\cdots\cdots\cdots\ (=1 \text{ と書きたい}) \\ 3-1=4-2=5-3=\cdots\cdots\cdots\cdots\ (=2 \text{ と書きたい}) \\ 4-1=5-2=6-3=\cdots\cdots\cdots\cdots\ (=3 \text{ と書きたい}) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{array}\right\} \longleftarrow \text{自然数！}$$

$\boldsymbol{a=b}$ **のとき**は

$$1-1=2-2=3-3=\cdots\cdots\cdots\cdots\cdots\cdots\ (=\ ?\ ) \quad \longleftarrow \quad 0 \text{ か？}$$

$\boldsymbol{a<b}$ **のとき**は

$$\left.\begin{array}{l} 1-2=2-3=3-4=\cdots\cdots\cdots\cdots\cdots\cdots\ (=\ ?\ ) \\ 1-3=2-4=3-5=\cdots\cdots\cdots\cdots\cdots\cdots\ (=\ ?\ ) \\ 1-4=2-5=3-6=\cdots\cdots\cdots\cdots\cdots\cdots\ (=\ ?\ ) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{array}\right\} \longleftarrow \text{負の整数？}$$

だが、ここで「 異なるかも知れない数 」を等号でつないでいるわけは、$a,\ b,\ u,\ v$ を自然数として

$$\boldsymbol{a-b=u-v} \iff \boldsymbol{a+v=u+b} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

である．つまり、自然数の「引くことで等しい」関係を、自然数の「足すことで等しい」関係から説明したものである と思ってもらえばよい．

たとえば、$a > b$ の例で、順序対 $(4,\ 1)$ と順序対 $(6,\ 3)$ が同じ数値であるのは

$$\overset{7}{\overbrace{4-1=6-3}}_{7} \quad \longleftarrow \quad 4+3=6+1\ (=7)$$

同様に、$a = b$ の例で、順序対 $(1,\ 1)$ と順序対 $(3,\ 3)$ では

$$\overset{4}{\overbrace{1-1=3-3}}_{4} \quad \longleftarrow \quad 1+3=3+1\ (=4)$$

また、$a < b$ の例で、順序対 $(1,\ 4)$ と順序対 $(3,\ 6)$ では

$$\overset{7}{\overbrace{1-4=3-6}}_{7} \quad \longleftarrow \quad 1+6=3+4\ (=7)$$

要するに、「 このような**順序対の存在**は**自然数の加法**によって保証されている 」のである．こうにして「 $\underbrace{a-b}_{\text{演算}}$ をドンドンやってできる数全体 」を全部ひっくるめて $\underbrace{\boldsymbol{(a-b)}}_{\text{集合}}$ と表すことにすると、この集合は事実上、私たちが普通に使い慣れているはずの**整数 $\boldsymbol{Z}$ の集合**になるであろう．

しかし、そうは言っても、この演算に現れるであろう **0** や**負の数**が、まだ説明されたわけではない——それらは、人々がその必要に迫られて作る出したもので、はじめから存在したわけではない．実は、**自然数**というときの「 **自然** 」というヒビキに対して、**0** や**負の数**はきわめて**作為的で人工的なもの**である．

そう思いつつ、$(*)$ で $\boldsymbol{a = b}$ とする．そうすると $u = v$ であるから

$$a-b=u-v=\text{ナシ} \quad \longleftarrow \quad \text{この段階で 0 (ゼロ) はまだ定義されていない！}$$

これを、具体的に書けば

$$1-1=2-2=3-3=\cdots\cdots\cdots\cdots\cdots\cdots=\ (\ ?\ ) \quad \longleftarrow \quad 0\text{ か？}$$

のことだが、ここには「 同じ数を引いたらなくなった 」という事実しかない．といって、ここに「 ナシ 」と書くわけにもいかず、何も書かなければ混乱する．

そこで、その「 **ナシ** 」を記述するための数として「 **0** 」という記号を導入する．つまり「 ない 」ことを「 0 」という記号で主張するのである——**0 の定義！**

ちなみに、この「 自然数に 0 が参加した集合 」においては

$$\text{加法：}\ a+0=0+a=a, \qquad \text{乗法：}\ a\cdot 0=0\cdot a=0$$

と決めると、この集合も**加法**、**乗法**について**閉じている**ことがわかる．

ここで、「 やっと **数 0** が定義できた 」から、この先は「 自然数に 0 が参加した集合 」で考えてもよいだろう——ここで、シツコクこだわるが、この「 **0** という数 」は、「 **負の数**を定義する 」ためには、「 **絶対に必要**な数 」なのである．

改めて $\boldsymbol{a > b}$ のとき、$(*)$ で $u = c,\ v = 0$ とおくと

$$a-b=c-0 \iff a+0=c+b$$

となる「 自然数 $c = 1, 2, 3, \cdots$ 」が必ずあり、その 1 つ 1 つに対して

$$\underbrace{(c-0)}_{\text{集合}}=\{1,2,3,\cdots\cdots\cdots\cdots\}=N$$

が決まるはずだから、これを改めて自然数とよぶことにすれば、自然数の集合 N は整数 Z の部分集合とみることができる——上記の「 書きたい 」の気持ちが説明できた.

これに対して、$\boldsymbol{a < b}$ のときは

$$a - b = 0 - c \iff a + c = 0 + b$$

となる「 自然数 $c = 1, 2, 3, \cdots$ 」が必ず存在し、「 $0 - c$ 」の「 $-c$ 」は自然数 c に記号「 $-$ 」がついたものだから、その 1 つ 1 つに対して決まる要素を表すために、**新しい記号**として、このカタチの通りに「 $\boldsymbol{0 - c = -1, -2, -3, \cdots}$ 」を導入する.

そうするとこの集合は

$$\underbrace{\boldsymbol{(0 - c)}}_{\text{集合}} = \{-1, -2, -3, \cdots\cdots\cdots\cdots\}$$

と表されるから、これを**負の整数**と決める——ココロでは順序対と読め！

結局、「 0 」は (ナシ) を、「 $-$ 」は (タリナイ分) を表す**タダの記号**と考えればよい. かくして、これらの和集合として、「 **正, 0, 負** 」の概念とともに、**整数全体の集合**が定義される. すなわち

$$\underbrace{\boldsymbol{(a - b)}}_{\text{集合}} = \begin{cases} a > b \text{ のとき} & \textbf{正の整数 (自然数)} \\ a = b \text{ のとき} & \boldsymbol{0} \\ a < 0 \text{ のとき} & \textbf{負の整数} \end{cases}$$
$$= \{\cdots\cdots\cdots, -4, -3, -2, -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ \cdots\cdots\cdots\}$$

である——**整数の集合**が定義できた.

ところで、整数の集合における**演算**はどうなっているのか. とりあえず、**加法**と**減法**については $a,\ b,\ c,\ d$ を自然数として

$$\textbf{加法：}\ \underbrace{(a - b)}_{\text{整数}} + \underbrace{(c - d)}_{\text{整数}} = \underbrace{(a + c)}_{\text{自然数 } a'} - \underbrace{(b + d)}_{\text{自然数 } b'}$$
$$= a' - b' \longleftarrow \textbf{順序対 } \boldsymbol{(a',\ b')} \in Z$$
$$\textbf{減法：}\ \underbrace{(a - b)}_{\text{整数}} - \underbrace{(c - d)}_{\text{整数}} = \underbrace{(a + d)}_{\text{自然数 } c'} - \underbrace{(b + c)}_{\text{自然数 } d'}$$
$$= c' - d' \longleftarrow \textbf{順序対 } \boldsymbol{(c',\ d')} \in Z$$

だから、何とか**閉じている**ことの説明がつく.

ここで、「 何とか 」というワケは、上の減法の場合、たとえば

$$(7 - 2) - \underbrace{(5 - 3)}_{A} = (7 + 3) - (2 + 5)$$

でいうと、問題はこの A の「 引く 3 」で、全体では A を引くのだが、その A では「 引く分が 3 だけ少ないのだから、先に足しておく 」というほどの意味である.

しかし、**乗法**についてはそう簡単にはいかない. とにかく**結論**から言うと、自然数の場合と同様に、というより経験的に

$$\boldsymbol{(a - b) \cdot (c - d) = (ac + bd) - (ad + bc)} \cdots\cdots\cdots\cdots\cdots (**)$$

となってくれないと困るのだ.

そこで、「 **自然数の場合の計算の形式** 」にしたがって展開すると

$$
\begin{aligned}
(a-b)\cdot(c-d) &= \underbrace{\{a+(-b)\}}_{M}\cdot\{c+(-d)\} \quad \longleftarrow \quad \textbf{第 1 分配則 を使う！}\\
&= \underbrace{\{a+(-b)\}}_{M}\cdot c+\underbrace{\{a+(-b)\}}_{M}\cdot(-d) \quad \longleftarrow \quad \textbf{第 2 分配則 を使う！}\\
&= ac+\underbrace{(-b)c}_{A}+\underbrace{a(-d)}_{B}+\underbrace{(-b)\cdot(-d)}_{C}\cdots\cdots\cdots(***)
\end{aligned}
$$

だが、ここで上記の $A,\ B,\ C$ はどうなるのか——「 負の数の絡んだかけ算 」はどう処理すればよいのか.

説明の途中で別件の証明はトートツでキブンが悪いがガマン——ともかく、それには $a>0,\ b>0$ として

$$
\boxed{\boldsymbol{(-a)b=a(-b)=-ab,\qquad (-a)(-b)=ab}}
$$

つまり、「 **(正) × (正) = (正)** 」は当たり前でよいが

$$
\textbf{(負)}\times\textbf{(正)}=\textbf{(負)},\qquad \textbf{(正)}\times\textbf{(負)}=\textbf{(負)},\qquad \textbf{(負)}\times\textbf{(負)}=\textbf{(正)}
$$

については説明しておかなくてはなるまい.

そこで改めて「 **負の数とは何か** 」を考えてみると

$$
\boldsymbol{a+x=x+a=0}\ \ (a>0) \quad \longleftarrow \quad \textbf{負の数の定義！}
$$

を満たす「 $\boldsymbol{x}$ 」のことである—— $\boldsymbol{-a}$ はこれを満たすから代入して

$$
\boldsymbol{a+(-a)=0} \ \longleftarrow\ \textbf{重要！}
$$

このことは何を意味するか——この式の $(-a)$ に注目してもらいたい.

上記の**負の数の定義**を、そのまま適用して読み換えると

$$
x+(-a)=0
$$

だが、上記によれば、これをを満たす x が $-(-a)$ だから、$\boldsymbol{a=-(-a)}$ である.

ところで、「 $\boldsymbol{b+(-b)=0}$ 」もいえるから、この両辺に a をカケルと

$$
ab+\underbrace{a(-b)}_{x}=0 \qquad \therefore\quad \underbrace{\boldsymbol{a(-b)}}_{x}\boldsymbol{=-(ab)}
$$

となり、同様にして $\boldsymbol{(-a)b=-(ab)}$ が示せるから、枠内の前半はカタがつく.

これだけの準備をすると、その結果が使えて

$$
\begin{aligned}
\boldsymbol{(-a)(-b)} &= -\{(-a)b\}=-\{-(ab)\}\\
&= \boldsymbol{ab} \quad \longleftarrow \quad \text{上記と同様に } \boldsymbol{ab+\{-(ab)\}=0} \text{ から言える！}
\end{aligned}
$$

である——**異符号の「 かけ算 」は負、同符号の「 かけ算 」は正**、とまとめておこう.

ともあれ、やっとのことで、この結果を $(***)$ に適用すると

$$
\begin{aligned}
\boldsymbol{(a-b)\cdot(c-d)} &= ac-bc-ad+bd\\
&= \underbrace{\boldsymbol{(ac+bd)}}_{\text{自然数 } k}-\underbrace{\boldsymbol{(ad+bc)}}_{\text{自然数 } l}\\
&= k-l \quad \longleftarrow \quad \textbf{順序対 } \boldsymbol{(k,\ l)}\ \in Z
\end{aligned}
$$

となり、整数の集合 Z は**乗法**についても**閉じている**ことがわかる———**整数**は、**加法**、**減法**、**乗法**の 3 法のすべてについて閉じているのである.

ちなみに、この途中で証明した

(マイナスの数) × (マイナスの数) = (プラスの数)

はなぜか、がよく話題になるが、上に説明したように、これは自然数で成り立つ計算をそのまま整数全体に拡張すると、それは**自動的に成り立つ結果**である.

つまり、それは「 整数 」というの集合の「 乗法 」という演算の中で、すでにその**属性**として確定している———数学としては当たり前のことなのである.

もっとも、現実の日常感覚にあわせた**説明のしかた**はいろいろあると思うから、やってみるとよい———つじつまの合うハナシで納得しておくとよい.

(注) 「 **0** 」や「 負の数 」は人間の知恵

0 はまだよいとしても、**負の整数の定義**にどうしてこんなタイヘンなことをするかというと、まだ -1 とか -2 とか、そういう負の数が一般に普及していない状態と思ってみればよい.

たとえば、3 個のりんごを 5 人の子どもに配るとしよう———トウゼン 2 個足りない. この状況を日常生活で切り抜けるには、「 足りない分は明日 …… 」とか、「 あとはツケということで …… 」などということになるだろう.

しかし、数学はそういうことは許さない———「 その足りない 2 個のりんごを出して見せろ 」と主張するわけである. しかし、まだ -2 という数が使えないから、「 それは $3-5$ です 」と、ありのままに見てもらうしかない. ところが、「 2 足りない 」場合は他にもあって、

$$1-3,\quad 2-4,\quad 3-5,\quad 4-6,\quad \cdots\cdots\cdots\cdots\cdots\cdots$$

など、いくつもある.

だが、これらを全部まとめて -2 と表すことにすれば、原始的な「 $a-b$ 」ようなヤボな表現をしなくてすむ. しかも、「 3 足りない 」、「 4 足りない 」…… などの場合も、これと同様に $-3,\ -4$ と表すことで、負の整数という概念が獲得できたのであろう.

そして、0 と自然数と合わせて、**整数**という、**減法**について**閉じている**集合が構成できる、とまあこんなハナシなのです.

かくして、人々は**負の数**を手に入れた. そして、**有理数** (分数)、**無理数**、そしてついには**虚数**と、数の範囲を拡張していくのである. しかし、実は、その拡張事業は虚数でオシマイである. このことはデカルトが証明している. レオポルト・クロネッカーという人の有名な言葉に

「 神は整数を作り給うた. 残りはすべて人間の業である.」

というのがある. 確かにそうかも知れないが、私たちの日常では「 -2 個のりんごをあげる 」とも言わないし、「 0 匹の魚を買いに行こう 」などと思う人もいない. 数学とは、そういう学問であるのか、と改めて考てみるとなかなか興味深い.

(注) ＜ end ＞

＜メモ＞

■ 改めて———「 整数 」は「 順序対 」である

本文の $(**)$ を見てもらいたい．それは

$$\boldsymbol{(a-b)\cdot(c-d)=(ac+bd)-(ad+bc)}\cdots\cdots\cdots\cdots\cdots(**)$$

のことである．そこで本文では 0 を定義し、負の数を定義し、それらの演算を定義して、それらを使って証明した———ひたすら自然数の加法をモデルにしてツジツマを合わせた格好だ．

しかし、もとをただせば $a-b$, $c-d$ は自然数の**順序対**、$(a,\ b)$, (c,d) のことであったはずである．たとえば $2\times3=6$ だが、この 6 は

$$(6=)\ \ 6-0=7-1=8-2=9-3=10-4=11-5=12-6=13-7=\cdots\cdots\cdots$$

のことであり、2 と 3 は

$$(2=)\ \ 2-0=3-1=4-2=5-3=6-4=7-5=8-6=\cdots\cdots\cdots$$
$$(3=)\ \ 3-0=4-1=5-2=6-3=7-4=8-5=9-6=\cdots\cdots\cdots$$

のことである．

そこで 2 と 3 を与える**順序対**を 1 つずつとって、**$(**)$ の右辺**を計算してみると、たとえば $(3,1)$ と $(4,1)$ でいくか．そうすると

$$\begin{aligned}2\times3&=(3-1)\cdot(4-1)\\&=(3\cdot4+1\cdot1)-(3\cdot1+1\cdot4)=13-7\ (=6)\end{aligned}$$

で、この結果が 6 を与える順序対の 1 つである $(13,\ 7)$ に対応していることがわかる———結局、2, 3 を与えるどの順序対の組み合わせに対しても、$(**)$ にしたがって計算する限り 6 を与える順序対のどれかに一致することが確かめられる．

本来はこういう計算結果からその一般の形である $(*)$ を誘導し**乗法**という演算を定義し、その上で分配則などを導くのが**スジ**というものであろう．

しかし、それではあまりに**タイヘン**である．そこで本文に述べたような方法をとったと考えてもらえばよい．

ここで、この立場から「 (負の数)×(負の数)=(正の数) 」を説明してみようか．

$$\underbrace{(0-2)}_{-2}\cdot\underbrace{(0-3)}_{-3}=\underbrace{(0\cdot0+2\cdot3)}_{6}-\underbrace{(0\cdot3+2\cdot0)}_{0}\quad(=6)$$

となり、これは整数に演算を設定した段階で、日常生活の感覚とは関係なく決定している**数学としての事実**である ことがわかる．こういうことの説明を

(借金) × (借金) = (大もうけ)

などと言い出すと、数学というより、もはや日常生活としても**意味不明**である———というより、上記の数学的事実を反映している実例ではないのだ．それを言うなら

今、数直線上を **時速 (-2)** で通過する点 P がある．**3 時間前** にはどこにいたか．

といこう———これなら計算の意味の説明になる．

つまり、時速 (-2) ということは左に動いているわけだから

$$(-2)\times(-3)=6$$

で、原点から **右に (プラス) 6** の地点にいたことになる———これならよい．いろいろ考えてみるとよい．

＜2＞「 有理数 」への拡張

(i)「 数の概念 」の拡張とその概要

整数と分数をまとめて**有理数**といい、これは英語の rational number の訳語である．この rational には「 合理的な 」という意味があるから、この訳が間違っているという訳ではないが、この語の**本来的な意味**は

比 (= ratio) に ナル (= nal) $\longleftarrow$ 冗談がキツイ！

ということで、「 有理数 」は、$\boldsymbol{m}$ を正の整数、$\boldsymbol{n}$ を任意の整数として

$$\boldsymbol{q = \frac{n}{m}}$$

で定義される．

そもそも、分数のルーツはどこにあるかというと、**連続量**、たとえば長さ、面積、体積、重さなどを扱うには、整数だけでは間に合わない．

それらを測るには、まず単位となる量が必要であり、その単位で測ったとき、それが必ずしも整数になるとは限らない．というより、ほとんどの場合にハンパが残る．

これを表現するためにはどうしても「 **分数** 」という考え方 が必要であった．したがって、分数が登場したのはかなり古い時代といわれている．

かの有名なピタゴラスは、自然数を万物の根源と考えていた．彼にとって

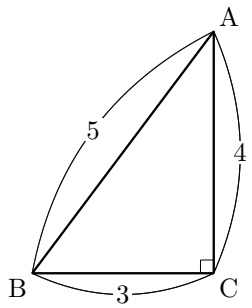
$$(\text{分数}) = \frac{(\text{自然数})}{(\text{自然数})}$$

で表される数は、いわば、自然数の従属物であった．そして、これだけですべての量を表しきれると考えていたのである．

一方、彼は**ピタゴラスの定理**の発見者とされているが、この定理の

$$3^2 + 4^2 = 5^2$$

という事実から、3 辺の比が $3:4:5$ になる三角形を作ると直角三角形になる．



$3^2 + 4^2 = 5^2$

3 辺がこの簡単な整数比で構成される美しい三角形は、ピタゴラスを満足させたようである．

しかし、そこには落とし穴があった．それは 2 辺が 1 の**直角二等辺三角形**の斜辺の長さ (今日、われわれは無理数、$\sqrt{2}$として知っている) を分数で表そうとしたとき、彼、あるいはその弟子たちは、それが不可能であることを発見するのである．これは、もはや教団ともいわれるほどの存在であったピタゴラスとその一派を根底からゆさぶった．

どんな小さな数直線上にも無限の分数がある．それなのに、それでも「 まだ数直線はビッシリと数でおおいつくされてはいない 」のだ．

これは、われわれの直感から言っても意外であるし、自然数をその土台におくピタゴラス的数学観にとって、その衝撃は大きかった．

これがピタゴラス教団が衰退する大きなキッカケになったといわれている．しかしこれは、数学の歴史の上では、「 **無理数** 」の発見そのものであった のである．

ともかく、ピタゴラスにとって、整数の比になる有理数はマコトに理にかなったことであり、そうならないことは不合理であったにちがいない．

そのあたりから rational という単語に合理的という意味が生じたのであろうか．今の私たちから見れば、「 もはや不合理ではなくなった数 」を「 無理数 」とよぶとき、好むと好まざるとにかかわらず、すでに「 ピタゴラス以来の歴史的な背景 」を背負わされてしまっているのである．

こういうハナシにくらべると、**負の数**の概念が確立されたのはずっと新しい．それへの準備に相当する期間を考えてれば、それはかなりさかのぼることにはなるだろうが、ともかく、「 負の数 」が「 **数** 」として承認され、実際の計算で使われるようになったのは 16 世紀になってからのことであると言われている．

そして、有理数も無理数も小数で表すことができて、これらは

有理数：有限小数または循環小数
無理数：　循環しない無限小数

となる．また、有理数の集合 Q は、0 で割ることを除いて**四則演算**（ **加法、減法、乗法、除法** ）について**閉じている**——これはあとで詳しく説明する．

しかし、無理数の集合は、この四則演算について閉じてはいない．反例をあげれば

$$(5+\sqrt{2})+(5-\sqrt{2})=10$$
$$\log 5+\log 2=1$$
$$(3+\sqrt{2})(3-\sqrt{2})=7$$
$$(2\pi)\div(\pi)=2$$

など、容易に思いつくだろう——「 有理数と無理数との和集合 」を**実数**という．

そして、実数の集合 R は 0 で割ることを除いて**四則演算**（ **加法、減法、乗法、除法** ）について**閉じている**

ここでは深入りはしないが、人々はやがて**虚数**という数の概念に到達する．この虚数 imaginary number は、**実数** real number に対立する言葉である．しかし、19 世紀に**複素数**の概念が確立したあとは、虚数も実数が real であるのと同じ程度に real になってしまった．それにもかかわらず、いまだに imaginary とよばれるのは、これもそのような歴史的事情によるものである．

そして、**虚数**の集合は四則演算について**閉じていない**．たとえば

$$(1+i)+(2-i)=3,\quad i\times i=-1$$

など、容易に反例を探すことができる．しかし、数の概念を虚数と実数の和集合である**複素数**にまで広げれば、四則演算について**閉じている**のである．

(注 1) 平方根 $\sqrt{(\quad)}$、そして虚数、複素数

ここでの話題は有理数だが、どうしても「 **無理数との境界** 」が問題になるので、無理数の典型的な例である平方根 $\sqrt{(\quad)}$ について触れておかねばなるまい．

たとえば、2 乗して 4 になる数は 2 つあって、それは 2 と -2 である．このとき 2 のことを $\sqrt{4}$ という——「 平方根 $\sqrt{(\quad)}$ 」は**正の数**のことをさしている のである．つまり

$$\sqrt{(\quad)} \geqq 0 \longleftarrow \text{ 等号は ( ) 内が 0 のとき！}$$

である．これを「 **根号の規約** 」というのだが、きわめて重要な意味を持っている．それは、この規約がなかったらどうなるかを考えてみればすぐにわかるであろう．

筆者は昔、高校生のとき

$$\sqrt{(-5)^2} = -5 \qquad (\longleftarrow \text{ 左辺は正 で 右辺は負 だからイコールのわけがないのだ！})$$

と書いて、「 これでどこが悪いのか 」と教師に質問したことがある．いろいろ説明してくれたが、何だかよくわからなかった．

実はこうである．

$$\sqrt{(-5)^2} = |-5| = -(-5) = 5 \longleftarrow \text{ これが正しい！}$$

としなければならないのだ——左辺に合わせて正になるように右辺の形を調整する のである．

これを、一般的な書き方で表せば

$$\boldsymbol{\sqrt{a^2} = |a| = \begin{cases} a \ (a \geqq 0\ ) \\ -a \ (a < 0) \end{cases}}$$

となる——ここまでは $\sqrt{(\text{正の数})}$ の場合のハナシだ．

$\sqrt{(\text{負の数})}$ のとき、これは**虚数**である——実数のときと扱いは全くちがうので、特に注意しなければならない．

結論からいうと、実数の集合に「 $\boldsymbol{i}$ 」という「 新しい数 」をつけ加えるのだが、そうすると、これらの間には**加、減、乗、除**の計算が今まで通りできると考える．

このとき、この i と実数の間は

$$i^2 = -1 \longleftarrow \boldsymbol{i = \sqrt{-1}} \text{ を 虚数単位 という！}$$

で結びつけられる．

このとき、$a,\ b$ を実数として

$$a + bi$$

で表される数を**複素数**といい、その中で、$b = 0$ のものを実数といい、$b \neq 0$ のものを**虚数**という．

また、複素数の集合は、0 で割ることを除けば**加法、減法、乗法、除法**について**閉じている集合**である．

また、$a > 0$ のとき

$$\boldsymbol{\sqrt{-a} = \sqrt{a}\sqrt{-1} = \sqrt{a}\ i}$$

と定める——これは**重要！**たとえば

$$\sqrt{-2}\sqrt{-3} = \sqrt{(-2)(-3)} = \sqrt{6} \qquad \longleftarrow (\ \times\ )$$

などとやってはならない．これをやるなら

$$\begin{aligned} \boldsymbol{\sqrt{-2}\sqrt{-3}} &= \boldsymbol{\sqrt{2}\ i \cdot \sqrt{3}\ i} \\ &= \boldsymbol{\sqrt{2} \cdot \sqrt{3} \cdot \underbrace{i^2}_{-1}} = \boldsymbol{-\sqrt{6}} \qquad \longleftarrow (\ \bigcirc\ ) \end{aligned}$$

としなければならない——とにかく、先に i で表して、あとは普通の文字計算をし、最後に i^2 を -1 に置き換えるのである．

この計算規則が確立したのは 19 世紀になってからのことといわれている．かのライプニッツ大先生でさえ、「 あの場合とか、この場合とか 」の条件つきで使っていたということである．

ちなみに、虚数には**大小関係**がない———大小関係とは「 $>$ 」、「 $=$ 」、「 $<$ 」のいずれか 1 つだけが成り立つことをいう．たとえば

$$i>0 \text{ とすると } i^2>0 \quad \therefore \quad -1>0 \quad (\times)$$
$$i=0 \text{ とすると } i^2=0 \quad \therefore \quad -1=0 \quad (\times)$$
$$i<0 \text{ とすると } i^2>0 \quad \therefore \quad -1>0 \quad (\times)$$

で、結局どの 1 つも成り立たないことから、「 **虚数には大小関係がない** 」———大小関係は実数を特徴づける重要な性質の 1 つである ということもできる．

＜ end. ＞

(注 2)　数の分類について

自然数に始まり、**整数**、**有理数**、**無理数**、**実数**、**虚数**、**複素数**と「 数の範囲 」を拡張してきたが、何のことやらわかりにくい．以下に図で示しておく．

- 複素数
  - 実数
    - 有理数
      - 整数
        - **正の整数（自然数）**
        - **0**
        - **負の整数**
      - 整数でない有理数 (分数)
        - 有限小数
        - 循環小数
    - 無理数 …… 循環しない無限小数 } 無限小数
  - 虚数

なお実数は、**(実数)^2 $\geqq$ 0** である．

＜ end. ＞

＜補足説明！＞

●「循環小数」と「鳩ノ巣原理」について

今この業界では「新課程には整数の分野が入る」とか、「入試には鳩ノ巣原理が出る」とか騒がれている．しかし、整数は小学校で始めて習いそれ以来トウゼンのように使っている数の概念だから入試ではそれとなく出ているから「何をいまさら」と思うし、鳩ノ巣原理にしても考え方そのものはアッタリマエのことだからそんなにトンガルことでもないと筆者は考えている．

とはいうものの、改めて入試の範囲などと言われると一応「それらしく」説明しておかなければなるまい．しかし、**鳩ノ巣原理**の説明が「なぜここか」と問われれば、上に述べた「**循環小数**の例」が身近の例として最もよかろう と考えるからである．以下に説明する．

まず「鳩ノ巣原理」だが、これは

「n 個の鳩ノ巣に $n+1$ 羽の鳩を入れようとすれば、必ずどれかの巣は 2 羽以上になる」

ということで、考えるまでもなくあたりまえのことである．

一般化すれば

「n 個の鳩ノ巣に m $(m > kn)$ 羽の鳩を入れる場合、必ずどれかの巣は $k+1$ 羽以上になる」

ということである———よく考えれば**あたりまえ**のことだ．

これを数学者のディレクレは引き出しにモノを入れる例で説明したらしく、ディレクレの引き出し論法とか部屋割り論法とか言われる場合もある．

ともあれ、これは「たくさんあるものの中で 2 つ (以上) は同じ」ことを証明するときなどに用いる証明の方法の 1 つとして知っておかねばならない重要な証明法の 1 つであると思えばよい．

ここでは、**循環小数の説明**としてきわめて重要 である．たとえば

「分数 (有理数) を小数で表す場合、それは有限小数か循環小数である」

ということを説明するには、まず分子を分母で割り、割り切れれば明らかに有限小数である．もし、割り切れなくて永遠に割り算が繰り返されるならばこれを循環小数というのである．

具体的に説明しよう．たとえば、分子を分母 n で割るとき得られる余りは $1,\ 2,\ 3, \cdots (n-1)$ であるがこれを**鳩ノ巣** とみよう．

今、割り算を n 回繰り返して余りが n 個得られたとする (**これが鳩**)．そうすると鳩ノ巣原理によれば、この余りのうち少なくとも 2 つは同じ数にならざるを得ない ということになる．

したがって、この計算では その同じ数に対応するところから小数は循環する ことになる．まあ、ざっとこんなところか．

筆者としては、高校数学ではこの循環小数を説明する場合の実用化ができればそれで十分と思うが、存在を証明する方法として**背理法**、**数学的帰納法**と並んで威力を発揮する場面が期待できる「論証の武器」ではある．これからはその目でながめておくとよい．

＜ end.＞

(ii)「 有理数 」とその計算の検証

改めて、**有理数**とは何か．**定義**によれば

$$\boldsymbol{q = \frac{n}{m}}, \quad \text{ただし } \boldsymbol{m} \text{ は正の整数, } \boldsymbol{n} \text{ は任意の整数}$$

で与えられる数が有理数である．

ここで、ちょっと注意しておかなければならないことがある．たとえば、2 つの集合を

$$A = \left\{ \frac{1}{2},\ \frac{2}{4},\ \frac{3}{6},\ \frac{4}{8},\ \cdots\cdots\cdots\cdots\cdots\cdots \right\}$$
$$B = \left\{ \frac{1}{3},\ \frac{2}{6},\ \frac{3}{9},\ \frac{4}{12},\ \cdots\cdots\cdots\cdots\cdots\cdots \right\}$$

とする．

まず、集合 A についていうと、これらの要素は「 個々に 」すべて**分数**である．約分するとすべて先頭の $\frac{1}{2}$ と等しくなるが、それぞれの「 **意味**するところ 」は

$\frac{1}{2}$ ⟵ 2 倍すると 1 になるもの！
$\frac{2}{4}$ ⟵ 4 倍すると 2 になるもの！
$\frac{3}{6}$ ⟵ 6 倍すると 3 になるもの！
$\frac{4}{8}$ ⟵ 8 倍すると 4 になるもの！
……
……

であるから、それぞれ「 ちがうもの 」と理解しなければならない．

一方、**ある有理数**という場合、たとえば集合 A でいうと、「 集合 A の分数のすべてをさしている 」わけで、この集合のどの要素を代表として選んでもよい——つまり、「 有理数 $\frac{1}{2}$ 」というのも「 有理数 $\frac{4}{8}$ 」というのも、どれを代表に選ぶかということだけのハナシで、結局は同じ結果になるのである．そして、それは集合 B についても同様である．

そして、小学生のときからおなじみの分数の**足し算**は

$$\boldsymbol{\frac{b}{a} + \frac{d}{c} = \frac{bc}{ac} + \frac{ad}{ac}} \quad \longleftarrow \quad \textbf{分母を揃えて通分する！}$$
$$\boldsymbol{= \frac{bc + ad}{ac}}$$

だが、これを上記の集合 $A,\ B$ の要素の間でやってみると、たとえば

$$\frac{1}{2} + \frac{1}{3} = \frac{3}{6} + \frac{2}{6} \quad \longleftarrow \quad \text{集合 } A,\ B \text{ の、「分母が同じもの」の足し算！}$$
$$= \frac{5}{6}$$
$$\frac{2}{4} + \frac{3}{9} = \frac{18}{36} + \frac{12}{36} \quad \longleftarrow \quad \text{集合 } A,\ B \text{ の、「分母が同じもの」の足し算！}$$
$$= \frac{30}{36} = \frac{5}{6} \quad \longleftarrow \quad \textbf{約分}\text{ したら上と同じ結果になった！}$$

ここで、$\dfrac{5}{6}$ を先頭にする集合 C を書いてみると

$$C = \left\{ \frac{5}{6},\ \frac{10}{12},\ \frac{15}{24},\ \frac{30}{36},\ \cdots\cdots\cdots\cdots\cdots\cdots \right\}$$

で、当然だがこの中には $\dfrac{30}{36}$ が入っている——ちょっとクドイが、**有理数の計算**とはこういうものなのです.

なお、集合 $A,\ B,\ C$ の先頭の数 $\dfrac{1}{2},\ \dfrac{1}{3},\ \dfrac{5}{6}$ のように、これ以上約分できない形の分数を**既約分数**というのである.

そして、これらそれぞれの集合の要素は約分すると同じ数値になるのだが、そのための条件を求めるには、その集合の 2 つの要素をとり出して、これを式で表すと

$$\boldsymbol{\frac{b}{a} = \frac{d}{c} \iff ad = bc \quad \therefore\ ad - bc = 0}$$

が成り立っている——実は、この**約束**のおかげで「 **有理数のすべての演算** 」がうまくいく ことになる——「 **数値として同等**である 」ことが担保される のである.

ともあれ、有理数の集合が**加法**について**閉じている**ことがわかった. **減法**についても、ほぼ同様であるから説明するまでもない——トウゼン**閉じている**.

さて、**乗法**についてはどう考えればよいか. たとえば

$$\frac{1}{2} \times \frac{1}{3} = \frac{1}{6} \ \longleftarrow\ \frac{1}{2}\text{を 3 等分すれば}\frac{1}{6}\text{になる！}$$
$$\frac{1}{2} \times \frac{5}{3} = \frac{5}{6} \ \longleftarrow\ \frac{1}{2}\text{を 3 等分したものが 5 個だから}\frac{5}{6}\text{になる！}$$

のように考えればよい——実際、ケーキでも買ってやってみればよい.

これを式で表すと

$$\boldsymbol{\frac{b}{a} \times \frac{d}{c} = \frac{bd}{ac}}$$

だが、これは問題なかろう——有理数は**乗法**について**閉じている**.

さて、**除法**についてはどうか. 小学校で「 **ひっくり返してかければよい** 」と習ったはずだ. つまり

$$\boldsymbol{\frac{b}{a} \div \frac{d}{c} = \frac{b}{a} \times \frac{c}{d}} \ \longleftarrow\ \text{割る方の分数}\frac{d}{c}\text{の分母子をひっくり返してかけた！}$$
$$= \frac{bc}{ad}$$

どうしてか——これはちょっとヤッカイだ.

具体的な例から入るのがよかろう. たとえば、「 5km を 40 分 で歩く人の時速を求めるにはどうすればよいか 」などがよいだろう.

時速を求めるのだから、40 分 を $\dfrac{2}{3}$ 時間と書き換えて

$$5 \div \frac{2}{3} = 5 \times \frac{3}{2} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$
$$= \frac{15}{2} = 7.5\ (\text{km/時間})$$

だが、$(*)$ の「 ひっくり返してかけた 」分数 $\dfrac{3}{2}$ の意味を考えてみてもらいたい.

歩いた時間は 40 分 だから、これを「 1 時間 (60 分) あたり 」に調整するわけである. つまり、「 $(*)$ の分数 $\dfrac{3}{2}$ 」の分母の 2 は 40 分の半分の 20 分で歩く分である.

そして、求めるものは 1 時間に歩く距離だから、その 3 倍ということだが、これを分子の 3 で表していると考えればよい.

公式を文字で表すとわかりにくいが、ハナシを簡単にするために、上記の公式で $\dfrac{b}{a} = A$ と書いておこう．そうすると

$$\begin{aligned} \frac{b}{a} \div \frac{d}{c} &= A \div \frac{d}{c} \quad \longleftarrow \quad \frac{b}{a} = A \\ &= \frac{A}{d} \times c = A \times \frac{c}{d} \end{aligned}$$

だから、先に d で割って「 **基本単位 $\boldsymbol{\dfrac{A}{d}}$ (この例では 20 分あたりの距離)** にしたものを **$\boldsymbol{c}$ 倍 (個数分)** する 」と考えるのである.

そういうわけで、有理数の集合は**四則演算**について**閉じている**ことがわかる．ただし、除法については 0 を除くものとする.

＜メモ＞

■「 無理数 」の存在を検証する

「 有理数でない無理数というものがある 」といわれても、実際にこの目で確かめないことには実感できないだろう．そこで、例題を 1 つやっておこう．

＜ 例 1 ＞

$\sqrt{3}$ が無理数であることを証明せよ．

(解) **背理法**で証明する———無理数であることをいうには、有理数であると仮定して矛盾が起こることをいえばよい．

$\sqrt{3}$ が 有理数であると仮定すれば

$$\boldsymbol{\sqrt{3} = \frac{n}{m}} \quad \longleftarrow \quad \textbf{既約分数！}$$

とおくことができる．そこで、分母を払うと

$$\sqrt{3}m = n \qquad \therefore \quad n^2 = 3m^2 \cdots\cdots ①$$

ここで、n が 3 の倍数であることはすぐにわかるが、ここは練習だから厳密にやろう———もう 1 度**背理法**を使えばよい．

n が 3 の倍数でないと仮定すると

$$n = 3k \pm 1$$

$$\therefore \quad n^2 = (3k \pm 1)^2$$

$$= 9k^2 \pm 6k + 1 = 3(3k^2 \pm 2k) + 1 \quad \longleftarrow \quad 3 \text{ の倍数でない！}$$

ゆえに n は 3 の倍数だから、$n = 3k$ とおいて ① に入れると

$$(3k)^2 = 3m^2 \qquad \therefore \quad m^2 = 3k^2$$

ゆえに、n の場合と同じ理由で m も 3 の倍数であるから、与えられた分数 $\dfrac{n}{m}$ が**既約分数**であるという 条件に**矛盾する**．

よって、$\boldsymbol{\sqrt{3}}$ **は有理数ではない**．すなわち**無理数**である．と、まあこんな具合にやればよい．とにかく実際に、有理数でない「 **無理数という数**の存在 」が確認された．

＜ end. ＞

■ 守備領域の確認

指数の拡張のハナシを思い出してもらいたい．指数法則は

$$a^m \times a^n = a^{m+n} \cdots\cdots ①$$

$$a^m \div a^n = a^{m-n} \cdots\cdots ②$$

$$(a^m)^n = a^{mn} \cdots\cdots ③$$

で、最初の条件は $m,\ n$ は整数で、$m > 0,\ n > 0,\ m > n$ であったはずだ．しかし、これらが「 すべての有理数 」で成り立つようにしないと不便で仕方がない．そこで、指数の範囲を拡張することにする．

② で $m = n$ でも成り立つようにするにはどうすればよいか．それには、まず、$m = n$ とおいてみる．すなわち

$$a^n \div a^n = a^{n-n} \qquad \therefore \quad a^0 = 1 \text{ とキメル} \quad \longleftarrow \quad \textbf{0 乗の定義！}$$

そこで、① で $m = -n$ とおいてみると

$$a^{-n} \times a^n = a^{-n+n}\ (= a^0 = 1) \qquad \therefore \quad a^{-n} = \frac{1}{a^n} \text{ とキメル} \quad \longleftarrow \quad \textbf{マイナス乗の定義！}$$

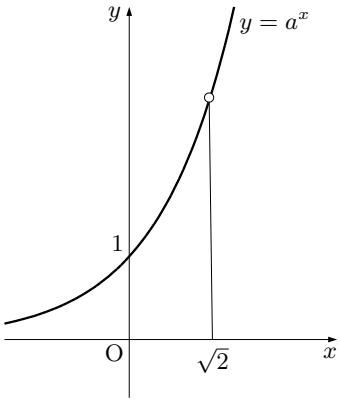
次に、③ で $m = \dfrac{1}{n}$ とおくと

$$(a^{\frac{1}{n}})^n = a^{\frac{1}{n}\cdot n} = a \qquad \therefore \quad a^{\frac{1}{n}} = \sqrt[n]{a} \text{ とキメル} \quad \longleftarrow \quad \boldsymbol{\frac{1}{n}} \textbf{乗の定義！}$$

また、③ で、n を $\dfrac{1}{n}$ に置き換えると

$$(a^m)^{\frac{1}{n}} = a^{m\cdot\frac{1}{n}} \qquad \therefore \quad a^{\frac{m}{n}} = \sqrt[n]{a^m} \text{ とキメル} \quad \longleftarrow \quad \textbf{有理数乗の定義！}$$

のように、次々と a^x の指数 x の範囲が拡張されていく．



しかし、ここで、中間テストや期末テストを思い出してもらいたい.

$$\boldsymbol{a^{\frac{1}{2}} \times a^{\frac{1}{3}} = a^{\frac{1}{2}+\frac{1}{3}}} \qquad \longleftarrow \text{ 指数は有理数！}$$

などが出た記憶はあるとおもうが

$$a^{\sqrt{2}} \times a^{\sqrt{3}} = a^{\sqrt{2}+\sqrt{3}} \longleftarrow \text{ 指数は無理数！}$$

などは見たことがないはずだ.

実いうと、高校数学では、「指数の拡張は有理数まで」で、無理数の場合は定義されていない のです.

だから、$y = a^x$ のグラフを描いても、x が無理数のところは定義されていないから、実は抜けていて、本当は隙間だらけのボコボコのグラフなのである.

それではあんまりだから、教科書も黒板もあたかもツナガッテイルように描く. まあ、今はよいとして、いつか埋めなければならないところがある、ということは知っておいたほうがよいでしょう———**実数の連続性**というテーマで大学でやります.

ちなみに、高校では数 III になると、「 そんなことは、まるでなかったかのように 」、全部ツナガッテイルことにして**微積分**をやるのです.

1.1.2　p 進法

われわれの日常生活で使っている数の表し方は、10 になると位が 1 桁あがるもので、**10 進法** といわれているものである．

たとえば、345 と表示された数は $3 \times 4 \times 5$ ということではなくて

$$\mathbf{3 \cdot 10^2 + 4 \cdot 10 + 5} \longleftarrow \ 10^2 = 100,\ 10,\ 1 \text{ がそれぞれ } 3,\ 4,\ 5 \text{ 個！}$$

のこと、すなわち、**10 を基準とした表し方 (記数法)** である．

しかし、記数法は 10 進法だけではなく、たとえば、時間の場合は 60 秒が 1 分、60 分が 1 時間で、60 ごとに位が 1 つ上がる 60 進法を用いている．これは角を測る単位として、1 度、1 分、1 秒でも用いられ、$1^\circ = 60'$,　$1' = 60''$ である．

この 60 進法は、バビロニアで多く用いられていたといわれているが、角を測る単位の関係もバビロニアに起源するものらしい．しかし、この 60 進法がなぜバビロニアに生まれ、使われたかはハッキリしない．

一説によれば、バビロニアは多くの小さな村落が寄り集まって次第に大きくなり、1 つの国家を形成するのだが、そのとき、各地方の度量衡を統一する必要が起こってきた．

そのためには多くの約数を持つ 60 という数が便利であった、というものである．たとえば、10 進法の国と 12 進法の国が統合されて新しい国を作るとすれば、10 でも 12 でも割り切れる数、10 と 12 の最小公倍数である 60 を基にして、60 進法にしておけば、その両方の国に都合がよいだろうというのである———まあ、もっともらしいが本当の理由はわからない．

おそらく、古代にはいろいろな「 数を数える仕組み 」があったであろう．しかし、どの場合もその底数 (基準となる数) が 10 に落ち着く傾向が強いようである．

その理論的な根拠があるわけではないが、これは、人間がいつも持ち歩いている計算の道具、すなわち **手の指が 10 本** だからである、という説明がそれなりの説得力を持つかに思われる．他に何か適当なものがあれば別の底数になる可能性もあったはずだ．

よく度量衡の単位にみられる例だが、たとえば、物の長さを測るとき、人間の体に備わった尺度として、指の長さ、ひじの長さ、歩幅などを使ったりするのは、ごく自然であったかと思われる．

$$1 \text{ yard} = 3 \text{ feet},\quad 1 \text{ foot(feet)} = 12 \text{ inches}$$

などはそういう名残りであろう．

一般に、度量衡の単位の間には、2, 3, 4 やその倍数が多いが、それは、長さ、容量、重量などが 2 分、3 分、4 分される必要があったためではないか．

ことに貨幣の単位に関しては 2, 3, 4 などの等分ができることが望ましい———**ワリカン**の都合を考えてみれば明らかだろう．そうなると、$\dfrac{1}{3}$ などは 10 進法の有限小数では表せないから却下ということになる．

バビロニアの 60 進法がどのように形成されたかを詳しく知る由もないが、10 進法の手の指による計算システムと、2, 3, 4, 6, 12 などを分母とする分数計算のシステムの統一過程と考えると、まあ、それなりに納得はできそうである．

しかし、60 進法で「 かけ算 」の「 九九 (くく) 」をやるとなると、これはタイヘンだ———$59 \times 59 = 3481$ 個の数を覚えなければならない．

それでも商人たちは「 九九表 」を作って商いをした、というハナシをどこかで読んだことがあるが、こうなるとあまり実用的ではない.

最近はコンピューターが大活躍だが、**コンピューター**の計算は 2 進法である.「 信号アリ 」を **1** とし、「 ナシ 」を **0** とすればよいのだから、機械的にも電気的にも、その基本原理はシンプルである——これにはいささか感動したことがある.

こうなると、あとはスピードの問題だけであるが、今や超高速の CPU やマザーボード、その周辺機器も開発され、およそ人間にかかわるありとあらゆるところで人々をサポートするにいたっている——これナシではもはや日常が成り立つまい.

改めて、その 2 進法だが、2 進法なら、そこに現れる数字は 0 と 1 だけであるから「 たし算 」も

$$\begin{array}{r} 0 \\ +\ \ 0 \\ \hline 0 \end{array} \qquad \begin{array}{r} 1 \\ +\ \ 0 \\ \hline 1 \end{array} \qquad \begin{array}{r} 0 \\ +\ \ 1 \\ \hline 1 \end{array} \qquad \begin{array}{r} 1 \\ +\ \ 1 \\ \hline 10 \end{array}$$

の 4 つしかない.

また、「 かけ算 」の「 九九表 」も、その結果は 4 つしかないから、計算の嫌いな人には魅力的である.

偉大な哲学者で数学者であった**ライプニッツ** (1646〜1716) は、熱心にこの 2 進法の利用を主張したといわれている.

	0	1
0	0	0
1	0	1

実用的には、それぞれ一長一短であるが、しかし、理論的には何進法であってもその**基本原理**は同じで、一般に p 進法 ($p \geqq 2$) の数を考えることができる.

(注) 「 位取り記数法 」と「 **0 という数** 」の存在について

ここで 1 つ、重要な指摘をしておかなければならない．ここで注目してもらいたいのは、「 位取り 」の方ではなくて、実は「 **0 という数** 」の存在なのである———もし、これがなかったらどうなるか．

具体的な例でいこう．たとえば、メロンの出荷で、まず、2 個ずつ桐の箱に入れるとする．さらにその箱を 2 個ずつダンボールの箱につめる．そしてダンボールを 2 個ずつ台車に乗せて運ぶ．次に台車 2 台分を軽トラックに乗せる．‥‥‥‥‥‥‥‥‥、などという状況を考えてみる．

上記の右端の「 たし算 」は、「 1+1 」で 2 つのメロンを桐の箱につめたとことである．この状態は個数で言えば 1 個だがそれは桐の箱分の 1 個だから、これはメロン 1 個のときの 1 とはちがう．さりとてバラのメロンはなくなったから (ナシ) ともかけない．「 **0 という数** 」はその「 (ナシ) 」を表していて「**桁上がり**」にはなくてはならない役割を担っている のである．

上記の場合は 2 進法だが、たとえば「 1001 」ならば、運搬の台車で 1 台分、ダンボールと桐の箱がともに 0 個 (ナシ) で、単体のメロンが 1 個ということがすぐにわかる．

もう 1 つ例を挙げておこう．たとえば、みかん 30 個をダンボールにつめる．ダンボール 50 個をトラックに載せる、トラック 100 台分を船に乗せる ‥‥‥‥‥‥‥‥‥、となると、ちょっと事情がちがってくる———現場監督は 30 個を、トラックの運転手はダンボールの個数を、船長はトラックの台数を管理すればよいわけだが、それぞれのレベルで基準がちがうので 1 つ 1 つの桁上がりがヤッカイだ———統一されていたほうがよいに決まっている．それにそれぞれの数値も大きすぎる．

日本の「 一、十、百、千、万、億、‥‥‥ 」などもこの手のものだが、なぜか 10 進法を基準しているのでいくらかは救われるが、「 尺貫法 」などはもう若い人にはわかるまい．

ヨーロッパではこの辺はずっと遅れていて、いまだに統一されていないという．そういう中で、ナポレオンが圧倒的に戦争に強かったのは「 メートル法 」を採用していたからだ、というのを聞いたことがあるが、妙に説得力がある．

まあ、大きな数を扱うにも小さな数を扱うにも 10 進法あたりがよかろうとこれに落ち着いて、今日に至っているのであろう．機会があったらいろいろ調べてみるとよい．

(注) ＜ end. ＞

1.1.2.1　p 進法による n 桁の表示

$\boldsymbol{p}$ **進法** の「 **記数表示** 」の**構造**がどうなるのかを知るために、まず、10 進法の表示で表された数の構造を眺めるところからはじめよう．

もう説明するまでもないが

$$3\text{ 桁} \longrightarrow a_1 \cdot 10^2 + a_2 \cdot 10 + a_3$$
$$4\text{ 桁} \longrightarrow a_1 \cdot 10^3 + a_2 \cdot 10^2 + a_3 \cdot 10 + a_4$$

であり、$a_1,\ a_2,\ \cdots$ は 0 から 9 の数だが、首位の a_1 だけは 0 を除くから

$$1 \leqq a_1 \leqq 9, \quad 0 \leqq a_2,\ a_3,\ a_4 \leqq 9$$

である．こう考えると、10 進法で表された n 桁の整数 $\boldsymbol{N = a_1 a_2 \cdots a_{n-1} a_n}$ は

$$\boldsymbol{N = a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots\cdots + a_{n-1} \cdot 10 + a_n}$$
$$(\text{ ただし、 } 1 \leqq a_1 \leqq 9, \quad 0 \leqq a_2, \cdots\cdots a_{n-1}, a_n \leqq 9 \text{ })$$

である――これは、まず問題なかろう．

そうすると、p 進法なら、上記の 10 の代わりに p と置き換えて

$$\boldsymbol{N = a_1 \cdot p^{n-1} + a_2 \cdot p^{n-2} + \cdots\cdots + a_{n-1} \cdot p + a_n}$$
$$(\text{ ただし、 } 1 \leqq a_1 \leqq p-1, \quad 0 \leqq a_2, \cdots\cdots a_{n-1}, a_n \leqq p-1 \text{ })$$

ということになり、これを簡単に

$$\boldsymbol{N = a_1 a_2 \cdots a_{n-1} a_n\ {}_{(p)}}$$

と表して、これを N の $\boldsymbol{p}$ **進記数法** というのである．

この場合、p 進法で用いられる数字は $0,\ 1, \cdots\cdots, p-1$ の p 個で、p 進法で n 桁の数の最小のものは p^{n-1} だから、N は

$$p^{n-1} \leqq N < p^n$$

の範囲にある．したがって、このような整数は全部で $p^n - p^{n-1} = p^{n-1}(p-1)$ 個あることになる．しかし、筆者は昔、ここを文字で書かれるとわかりにくかった．

だから、10 進法で、たとえば 3 桁の数は 100, 101, 102, $\cdots\cdots$, 999 と確認して

$$\underbrace{100}_{10^2} \leqq (3\text{ 桁}) < \underbrace{1000}_{10^3}, \qquad 999 - 99 = 900\ (= 10^2 \cdot 9)$$

と、いつもこれをワキに書いて確かめたものである．

これは普段、10 進法にあまりに慣れ親しんでしまっているので、急に約束事を変えられることへの戸惑いである――読者もモタモタしたらやってみるとよい．

さて、**小数**のときはどうするか――やってみよう．たとえば、0.234 ならば

$$\frac{2}{10} + \frac{3}{10^2} + \frac{4}{10^3} \quad (\ = 2 \cdot 10^{-1} + 3 \cdot 10^{-2} + 4 \cdot 10^{-3}\ )$$

となる．

これと同様に考えて p 進法 の場合だと、たとえば小数の $ab.cde_{(p)}$ は

$$a \cdot p + b \cdot p^0 + c \cdot p^{-1} + d \cdot p^{-2} + e \cdot p^{-3}$$
$$= ap + b + \frac{c}{p} + \frac{d}{p^2} + \frac{e}{p^3}$$

となるのである．

1.1.2.2　p 進法表示で表された数を q 進法表示になおす

たとえば、5 進法の数 $4301.2_{(5)}$ を 10 進法になおすには

$$4 \cdot 5^3 + 3 \cdot 5^2 + 0 \cdot 5 + 1 \cdot 5^0 + 2 \cdot 5^{-1}$$

とすればよい.

それでは、10 進法で表された数 785 を 7 進法で表すにはどうすればよいか———これはちょっと難しい.

7 進法というのは 7 で 1 桁繰り上がり、さらにその桁の 7^2 で次に繰り上がり、それを繰り返すのだから、右に示すようなれ連続した割り算を実行すればよい.

$$\begin{array}{r|rcl} 7 & 785 & & \\ \hline 7 & 112 & \cdots & (1) \\ \hline 7 & 16 & \cdots & (0) \\ \hline & (2) & \cdots & (2) \end{array}$$

そうすると、最上段の余り (1) が末位の数、次の余り (0) が 7 の端数、その次の余り (2) が 7^2 の端数、最後の (2) が 7^3 の個数だから、7 進法の表示では、図の数値を最下段から右の余りへ、そして余りを上へと読んで、 $2201_{(7)}$ となる.

つまり、この割り算は

$$2 \cdot 7^3 + 2 \cdot 7^2 + 0 \cdot 7 + 1 = 2201_{(7)}$$

で、7 進法の「 組み立て 」そのものを表していることがわかるであろう.

一般に、10 進法の数を N として、N を順次 q で割った余りをその右に書き、商が q より小さくなるまでこれを続ける.

商が q より小さくなったところでこの計算をやめるのだが、それが右のようになったとすると、この累進表示は

$$\begin{array}{r|rcl} q & N & & \\ \hline q & N_1 & \cdots & \alpha_1 \\ \hline q & N_2 & \cdots & \alpha_2 \\ \hline & \alpha_4 & \cdots & \alpha_3 \end{array}$$

$$N = \alpha_4\alpha_3\alpha_2\alpha_1$$

となる.

つまり、N の先頭からの順序は右の計算のシッポから書くのである. その理由は、計算過程を 1 つ 1 つ調べていくと

$$N = qN_1 + \alpha_1, \quad N_1 = qN_2 + \alpha_2, \quad N_2 = q\alpha_4 + \alpha_3$$

だから、順次代入して

$$\begin{aligned} N &= q(qN_2 + \alpha_2) + \alpha_1 = q^2N_2 + q \cdot \alpha_2 + \alpha_1 \\ &= q^2(q\alpha_4 + \alpha_3) + q \cdot \alpha_2 + \alpha_1 \\ &= \boldsymbol{\alpha_4 \cdot q^3 + \alpha_3 \cdot q^2 + \alpha_2 \cdot q + \alpha_1} \\ &= \boldsymbol{\alpha_4\alpha_3\alpha_2\alpha_1}_{(q)} \quad \longleftarrow \quad q \text{ 進法表示！} \end{aligned}$$

となるからである.

以上のことから、p 進法で表された数を q 進法で表すには、まず 10 進法になおし、その上でそれを改めて q 進法になおせばよいということがわかる.

(注) 小数の場合——これは知っておいてもよい.

たとえば、$0.26_{(8)}$ を 6 進法になおしてみよう——まず 10 進法表示になおし、その上で 6 進法で表示するという手順になる.

10 進法で表示するには

$$\begin{aligned} 0.26_{(8)} &= \frac{2}{8} + \frac{6}{8^2} \\ &= 0.25 + 0.09375 = 0.34375_{\ (10)} \end{aligned}$$

で、これは問題なかろう. そこで、この 0.34375 を 6 進法で表示するには、まず

$$0.34375 = \frac{a_1}{6} + \frac{a_2}{6^2} + \frac{a_3}{6^2} + \cdots\cdots\cdots$$

<u>この 両辺を **6** 倍する</u> と

$$2.0625 = a_1 + \frac{a_2}{6} + \frac{a_3}{6^2} + \cdots\cdots\cdots \qquad \longleftarrow \quad 0.34375 \times 6 = 2.0625$$

両辺の**整数部分を比較**して

$$a_1 = 2$$

$$\therefore \quad 0.0625 = \frac{a_2}{6} + \frac{a_3}{6^2} + \cdots\cdots\cdots$$

<u>これを 6 倍する</u> と

$$0.375 = a_2 + \frac{a_3}{6} + \frac{a_4}{6^2} + \cdots\cdots\cdots \qquad \longleftarrow \quad 0.0625 \times 6 = 0.375$$

両辺の整数部分を比較して

$$a_2 = 0$$

$$\therefore \quad 0.375 = \frac{a_3}{6} + \frac{a_4}{6^2} + \cdots\cdots\cdots$$

<u>さらに 6 倍して</u>

$$2.25 = a_3 + \frac{a_4}{6} + \cdots\cdots\cdots \qquad \longleftarrow \quad 0.375 \times 6 = 2.25$$

だから、両辺の整数部分を比較して $a_3 = 2$ を得る.

以下、これを繰り返して

$$0.26_{(8)} = 0.20213_{(6)}$$

が得られる.

まあ、結果はこういうことだが、場合によると、どこまでやっても終わらないときもあるのでヤッカイだ. たとえば $0.26_{(10)}$ を 5 進法の小数になおすと

$$0.26_{(10)} = 0.11222\cdots_{(5)} = 0.11\dot{2}_{(5)}$$

つまり、循環小数になるのである.

(注) ＜ end. ＞

＜メモ＞

■ $\boldsymbol{p}$ 進法の実際

$\boldsymbol{p}$ **進法**についての基本的な考え方についてはすでに述べたが、実を言うとあまりピンとこないであろう———筆者もそうなのだから心配しなくてよい．

それは、「 私たちの日常は余りにも 10 進法に慣れてしまっている 」ので、突然 5 進法とか 7 進法とかいわれても、心理的についていけない のである．

10 進法はそれほど深くわれわれの生活に浸透しているのである———このことのほうが**スゴイ**とは思わないか．人々の暮らしは何千年もその中でドップリ成り立ってきたのである．いまさら突然そういわれても困るに決まっている．

そういうときは、まず慣れている「 10 進法の構造 」がどうなっているかを考え、それにならって「 新たに**位取り記数法**を構成する 」ほどの覚悟が必要である———やってみればわかるが、慣れないと相当にヤッカイなのだ．まずは 10 進法の例から説明しよう．

＜ 例 1 ＞

10 進法で表された 3 桁の整数がある．各位の数の和が 9 で割り切れるなら、その数は 9 で割り切れる．これを証明せよ．

(解) 与えられた 3 桁の整数 N を

$$\begin{aligned}\boldsymbol{N} &= \boldsymbol{a\cdot 10^2 + b\cdot 10 + c} \quad (\ 1 \leqq a \leqq 9,\ \ 0 \leqq b,\ c \leqq 9\ ) \\ &= 100a + 10b + c\end{aligned}$$

とおいて、各位の数の和をとり出す工夫をする．すなわち

$$\begin{aligned}N &= (a+b+c) + (99a+9b) \quad \longleftarrow \quad (a+b+c) \text{ をとり出して分離！} \\ &= (a+b+c) + \underbrace{9(11a+b)}_{9\text{ の倍数}}\end{aligned}$$

となり、$a+b+c$ が 9 で割り切れるならば N は 9 で割り切れる．

コトのついでに、$a+b+c$ が 3 で割り切れるならば N が 3 で割り切れることもわかる．

★ 一般の場合に拡張する．

上に述べたハナシは、一般に n 桁の整数についていえることがらである．

$$\begin{aligned}N &= a_1\cdot 10^{n-1} + a_2\cdot 10^{n-2} + \cdots\cdots + a_{n-1}\cdot 10 + a_n \\ &\qquad (\ \text{ただし、}\ 1 \leqq a_1 \leqq 9,\quad 0 \leqq a_2, \cdots\cdots a_{n-1}, a_n \leqq 9\ )\end{aligned}$$

とおくと、上の 3 桁の場合と同様に

$$N = (a_1 + a_2 + \cdots + a_n) + \underbrace{\{a_1(10^{n-1}-1) + a_2(10^{n-2}-1) + \cdots + a_{n-1}(10-1)\}}_{A}$$

ここで $10^{k-1}-1$ を因数分解すると

$$\begin{aligned}10^k - 1 &= (10-1)(10^{k-1} + \cdots + 10 + 1) \\ &= 9(10^{k-1} + \cdots + 10 + 1)\end{aligned}$$

となり、上記の A の部分はどの項も 9 で割れることがわかる．

したがって、各位の数の和 $(a_1 + a_2 + \cdots + a_n)$ が 9 で割れるならば N も 9 で割り切れる のである．なお、この性質は 3 で割り切れる場合も含めて**定理**として用いてよい．

＜ end. ＞

10 進法の問題をもう 1 つやっておく.

＜例 **2**＞

ある正の整数の 1 位の数の 5 倍と、その 1 位の数字を消して得られる数 (たとえば 765 であれば 5 を消して 76) との差が 17 の倍数のとき、はじめの整数も、また 17 の倍数である.
このことを証明せよ.

(解) 特にことわりがないから、この数 N は 10 進法で表されていると考えてよい. すなわち

$$N = a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots\cdots + 10 \cdot a_{n-1} + a_n$$
$$(\text{ ただし、 } 1 \leqq a_1 \leqq 9, \quad 0 \leqq a_2, \cdots\cdots a_{n-1}, a_n \leqq 9 \text{ })$$

そこで、問題になっているのは 1 位の数だから

$$N = 10\underbrace{(a_1 \cdot 10^{n-2} + a_2 \cdot 10^{n-3} + \cdots\cdots + a_{n-1})}_{M \text{ とおく}} + a_n \quad \longleftarrow \text{ 簡単にまとめる！}$$
$$= 10M + a_n$$

そうすると、問題文の「1 位の数を消して得られる数」というのは上記の M そのものである.
よって条件は

$$M - 5a_n = 17k \qquad \therefore \quad M = 5a_n + 17k$$

これを入れると N は

$$\begin{aligned} N &= 10M + a_n \\ &= 10(5a_n + 17k) + a_n \\ &= 51a_n + 170k = 17(3a_n + 10k) \quad \longleftarrow \textbf{ 17 の倍数！} \end{aligned}$$

となり、証明された.

＜ end. ＞

＜例 **3**＞

7 進法で表された次の 2 数の計算結果を 5 進法で表せ.

(1) $256 + 203$　　(2) $1024 - 566$　　(3) 306×42　　(4) $651 \div 21$

(解) 7 進法や 5 進法を扱うときは、10 進法のときのようにうまくいかない———10 進法の感覚に振り回されるのである.
そういうときは、<u>**演算表**を作って、1 つ 1 つ確認しながら地道に進むしかない</u>.

(1) まず、7 進法の数の「 **加算の演算表** 」は右のようになる.

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	10
2	2	3	4	5	6	10	11
3	3	4	5	6	10	11	12
4	4	5	6	10	11	12	13
5	5	6	10	11	12	13	14
6	6	10	11	**12**	13	14	15

「 $256 + 203$ 」は、次のように計算する.
つまり

$$\begin{array}{r} 356 \\ +)\ 203 \\ \hline 562_{(7)} \end{array}$$

である. しかし、このまま**素手**ではやりにくい.
たとえば末位でいうと 10 進法なら「 $6 + 3 = 9$ 」だが、この場合 **7 進法**の計算だから 7 で 1 桁繰り上がることになる———まず、これがヤッカイだ.
さらに、末位は繰り上がった分を差し引いて「 $9 - 7 = 2$ 」としなければならない———そういう気遣いをせずに、ただ単純に、表を目で見てすぐにわかるように演算表を作るのである.
表でいえば、6 段目の右へ 3 つ数えた「 12 」という数がこれにあたると見ればよい. 他の場合も、こういう表を作っておいて、それを見ながら計算を実現すればよいワケである.
さて、ともかく計算の結果は $562_{(7)}$ となった.

次に、7 進法で表されたこの数を 5 進法に直すには、まず 10 進法にして、それから 5 進法にするという 2 重の手続きになる.

そこで、上記の結果を 10 進法に直すには

$$562_{(7)} = 5 \cdot 7^2 + 6 \cdot 7 + 2 = 289_{(10)}$$

$$\begin{array}{r|l} 5 & 289 \\ \hline 5 & 57 \cdots (4) \\ \hline 5 & 11 \cdots (2) \\ \hline & (2) \cdots (1) \end{array}$$

とすればよい. こうしておいて、やっと 5 進法に直す計算をするのである.

計算は前にも述べたが、右に示す割り算を実行して $2124_{(5)}$ が得られる———上に示した.

(2) 今度は「 引き算 」だが、これは 10 進法で「 上の桁から 10 をおろして $\cdots$ 」とやるところを、7 進法だから「 **上の桁から 7 をおろして** $\cdots$ 」としなければならない.

しかし、これはまたこれでうっとおしい.
そういうことなら、いっそ「 最初から 10 進法に直してしまう 」方がよさそうだ———慣れている分、速くて確実だろう.

$$2014_{(7)} = 2 \cdot 7^3 + 0 \cdot 7^2 + 2 \cdot 7 + 4 = 361_{(10)}$$

$$566_{(7)} = 5 \cdot 7^2 + 6 \cdot 7 + 6 = 293_{(10)}$$

$$\begin{array}{r|l} 5 & 68 \\ \hline 5 & 13 \cdots (3) \\ \hline & (2) \cdots (3) \end{array}$$

だから

$$361 - 293 = 68_{(10)}$$

さらに、これを 5 進法に直すと $233_{(5)}$ となる———上に計算を示しておいた.

(3) 7 進法の「 **九九表** 」を作る.

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	11	13	15
3	0	3	6	12	15	21	24
4	0	4	11	15	22	26	33
5	0	5	13	21	26	34	42
6	0	6	15	24	33	42	51

これを用いて「 かけ算 」をすると次のようになる.

$$\begin{array}{r} 306 \\ \times) \quad 42 \\ \hline 615 \\ 1533 \\ \hline 16245_{(7)} \end{array}$$

これを 5 進法に直せば $121330_{(5)}$ となるが、この計算はもういいだろう.

(4) これは、もう最初から 10 進法に直して計算する.

$$651_{(7)} = 6 \cdot 7^2 + 5 \cdot 7 + 1 = 330_{(10)}$$

$$21_{(7)} = 2 \cdot 7 + 1 = 15_{(10)}$$

そこで割り算を実行すると

$$330 \div 15 = 22_{(10)}$$

これを 5 進法に直す計算はやってください——— $42_{(5)}$ となる.

＜ end. ＞

＜例 4＞

次の文を読んで、あとの設問に答えよ．

「 k を 2 から 10 までの任意の整数とするとき、正の整数はすべて

$$a_n \times k^n + \cdots\cdots + a_1 \times k + a_0$$

と書くことができる．ただし、$a_0,\ a_1, \cdots, a_n$ を 0 から $k-1$ までの整数とする．

したがって、上の式で書かれる数を $a_n \cdots a_1 a_0$ のように、数字 $a_n,\ \cdots,\ a_1,\ a_0$ の単なる配列で表すことができる．そして、10 進法というのは、k を 10 にとったときのことであるが、k を 2 にとれば 2 進法といわれる記数法になる．」

(1) 10 進法で 365 と書かれた数を 2 進法で表せ．

(2) 2 進法で 101101 と書かれた数と 1011 と書かれた数との積を 2 進法で表せ．

(3) 正の整数 x が 2 進法で書かれているとき、それを右から 3 桁ずつ区切っていき、2 進法で各区切りを表す数 $y_0,\ y_1,\ \cdots\cdots,\ y_m$ を考える．もし、これらの和 $y_m + \cdots\cdots + y_1 + y_0$ が 7 で割り切れるなら、x も 7 で割り切れることを証明せよ．

(解) (1) まず、割り算を実行する———右に示す．

2	365		
2	182	$\cdots$	(1)
2	91	$\cdots$	(0)
2	45	$\cdots$	(1)
2	22	$\cdots$	(1)
2	11	$\cdots$	(0)
2	5	$\cdots$	(1)
2	2	$\cdots$	(1)
	(1)	$\cdots$	(0)

$$365 = 2^8 + 2^6 + 2^5 + 2^3 + +2^2 + 1$$

となり、したがって 2 進法で表すと $101101101_{(2)}$ となる．

(2) 2 進法では $1+1=10$ であるから、2 進法のままでやる．

$$\begin{array}{r} 101101 \\ \times)\quad 1011 \\ \hline 101101 \\ 101101 \\ 101101 \\ \hline 111101111_{(2)} \end{array}$$

だが、それぞれ 10 進法に直すと

$$101101_{(2)} = 2^5 + 2^3 + 2^2 + 1 = 45_{(10)}$$

$$1011_{(2)} = 2^3 + 2 + 1 = 11_{(10)}$$

だから、先に $45 \times 11 = 495$ を求めておいて、これを 2 進法で表して $111101111_{(2)}$ としてもよい———計算省略！

(3) 2 進法の数を末位から 3 つずつ区切るとき、現れる 3 つの数を、大きいほうから並べてみると

111, 110, 101, 100, 011, 010, 001, 000

の 8 通りが考えられるが、これらを 10 進法で表すと

$$111_{(2)} = 2^2 + 2 + 1 = 7$$

$$110_{(2)} = 2^2 + 2 + 0 = 6$$

$$101_{(2)} = 2^2 + 0 + 1 = 5$$

$$100_{(2)} = 2^2 + 0 + 0 = 4$$

$$011_{(2)} = 0 + 2 + 1 = 3$$

$$010_{(2)} = 0 + 2 + 0 = 2$$

$$001_{(2)} = 0 + 0 + 1 = 1$$

$$000_{(2)} = 0 + 0 + 0 = 0$$

で、これらは 0 から 7 までのどれかになっている．つまり、これらは 8 進法で表した記数表示の各桁の数字を表している———ここがおもしろいではないか．

また 2 進法で、1000 ; 1000000 ; $\cdots$ と表される数字は $2^3 = 8$; $2^6 = 8^2$; $\cdots$ であるから、x を 2 進法で表して右から 3 桁ずつ区切って、各区切りの表す数を $y_0, y_1, \cdots, y_m$ とすると

$$x = 8^m \cdot y_m + 8^{m-1} \cdot y_{m-1} + \cdots + 8 \cdot y_1 + y_0$$

$$\therefore \quad x - (y_m + y_{m-1} + \cdots + 8y_1 + y_0)$$
$$= (8^m - 1)y_m + (8^{m-1} - 1)y_{m-1} + \cdots + (8-1)y_1$$

ここで、一般に

$$8^k - 1 = (8-1)(8^{k-1} + 8^{k-2} + \cdots + 8 + 1)$$
$$= 7\,(8^{k-1} + 8^{k-2} + \cdots + 8 + 1) \quad \longleftarrow \quad \textbf{7 の倍数！}$$

となる．したがって、$y_m + y_{m-1} + \cdots + y_1 + y_0$ が 7 の倍数ならば x も 7 の倍数である．

★$_1$ 各位の数の和

前掲の＜例 1 ＞では 10 進法で、「 各位の数の和 」が 9 の倍数ならば、もとの数が 9 の倍数であることを確認した．本問は 8 進法の場合、「 各位の数の和 」が 7 の倍数ならば、もとの数が 7 の倍数である例である．

これは一般に拡張の場合にされて、p 進法では「 各位の数の和 」が $p-1$ の倍数ならば、もとの数が $p-1$ の倍数であることがいえる———知っておいてもよいハナシである．

★$_2$ 各位の数の和

前にも述べたが、コンピューターでは 2 進法を用いるのだが、たとえば

$$1974_{(10)} = 11110110110_{(2)}$$

のように表示が長くなって、ひと目でその数をとらえることが困難である．そこでコンピュータ語ではよく 8 進法が使われるのである．上記の例では、その長い数字の列を区切って

$$1974_{(10)} = 011,\ 110,\ 110,\ 110_{(2)} = 3666_{(8)}$$

のように書いたりする．

このことは 10 進法でも使っている．たとえば

$$8974321924 = 89,\ 747,\ 321,924$$

などだが、これは物理の「 MKS 単位 」のとり方に由来するものかと思われる———10 万円のところを 100k(k はキロ) 円と書いてあると何となく理科系的な気がしないでもない．

＜ end. ＞

1.2　整数入門———整除の定理

整除の定理などというと難しく感じるかも知れないが、A を B で割るとき、これを式で表すと $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ を整数として

$$\boldsymbol{A = BQ + R} \longleftarrow A \text{ を } B \text{ で割るとき、商 が } Q \text{ で 余り が } R \text{ のこと！}$$

と表される．上記は文字で書いたがわかりにくければ、これを具体的な数値で表すと、たとえば、178 を 7 で割るとすれば

$$178 = 7 \times 25 + 3 \longleftarrow 178 \text{ を 7 で割るとき、商 が 25 で 余り が 3 ということ！}$$

のように表す———この表現はあらためて説明するまでもなかろう．

しかし、この整除の定理はこのあと、整数のいろいろな性質を考える上できわめて重要な意味を持つことになる———個人的には、ここが**約数**とか**倍数**とかを含む**整数に関する諸問題**を扱う流れの**水源**である と思っている．

＜補足説明＞ 整除の定理、その守備領域について

本文では「**水源**」という言葉で表したが、こう書いたのでは「文学的?」に過ぎて何のことやらわからないかもしれない．個々についての詳しい解説は適宜に用意してあるが、まずは ザックリと全体の見方を先に書いておく 方がよさそうだ．

あらためて整除の定理は

$$\boldsymbol{A = BQ + R} \longleftarrow A \text{ を } B \text{ で割るとき、商 が } Q \text{ で 余り が } R \text{ の数式表現！}$$

だが、ここで $\boldsymbol{R = 0}$ とすると

$$\boldsymbol{A = BQ} \ (\text{ただし } \boldsymbol{B \neq 0}) \longleftarrow \boldsymbol{A} \text{ は } \boldsymbol{B} \text{ で割り切れる！}$$

つまり、言葉を変えれば「$\boldsymbol{A}$ は $\boldsymbol{B}$ の倍数である」、または「$\boldsymbol{B}$ は $\boldsymbol{A}$ の約数である」の問題になる———詳しくは後述するとして、約数、倍数はこの延長線上のハナシ なのだ．そして整数問題のシリアスな場面のほとんどはこれらの**意味の理解**と**使い方**にかかっていると思ってよい．

また、目先をかえて **余り** $\boldsymbol{R}$ に注目すれば、 $R = 0,\ 1,\ 2,\ \cdots\cdots,\ B-1$ だから 剰余類、合同式など、「余りの部分だけの計算」のハナシに展開 する．これも約数、倍数とはちがったカタチで**意味の理解**と**使い方**にかかっている．

まあ、どこから手をつければよいかに戸惑う「整数」ではあるが、まずは**整除の定理**を出発点として系統的にこれだけの広がりがあることを認識してもらいたい．

おそらく、これだけのことを正確にマスターするだけで、君たちが不得意とする整数の分野の相当深い所にまで切り込めるのではないかと思う．他にも**ガウス記号**など、君たちが嫌う分野もないではないが、それは個々に潰していけばよい．

＜ end. ＞

＜メモ＞

■ 入門テスト

あらためて思い返してもらいたい、小学生のときから約数とか倍数とかという言葉を用いてきたのだが、そして整数が数学の最も素朴な入り口であるはずなのだが、その**定義**さえ何となくハッキリしていない.

そこで、とりあえず**挨拶がわり**にナマの入試問題で**入門テスト**をやろうと思う．実際にハナシを展開する前に、どこまでが君のもので、どこからがまだ私のものか、お互いに状況を確認しておくことは良いことだ——ぜひ乗ってもらいたい．きっと新しい発見がある.

もし、知らないことがあったとしてもそれはそれでよろしい——新たに学べばよいだけのことである．ではさっそく始めよう.

＜例＞

次の文章により、整数についてのいろいろな**数学的概念**を**数学用語**で定義する.

「整数 a, b に対して、$\boldsymbol{a = bx}$ となる整数 x があるとき、a は b で**割り切れる**、または b は a の**約数**であるという.

また、いくつかの整数を同時に割り切れる整数をそれら**公約数**といい、公約数のうち最大のものを**最大公約数**という.

そして、1 より大きい整数がそれ自身と 1 以外に正の約数をもたないとき、それを**素数**といい、正の整数がそれ自身と 1 以外に正の約数をもつとき、それを**合成数**という．」

この定義にしたがって、次の (1)〜(5) の各々につき、それに当てはまる整数があればそれをすべて列挙し、なければ「ない」と書け.

(1) すべてが割り切れる整数
(2) 0 が割り切れない整数
(3) -1 と 0 との最大公約数
(4) 90 と 100 との間にある素数
(5) 素数でも合成数でもない正整数

(解) 問題文を見ると、文中に**数学的概念**やら**定義**やらがシッカリと書き込まれている．この手の出題形式の問題を扱うには、一般の通念というか日常に使い慣れている数学的概念を捨てて、あくまで上記の**ワクの中の約束事**の制限のもとに思考を進めなければならない——読んだことをそのままストレートに受け入れる素直さが必要である.

まず、本文で与えられた等式を

$$\boldsymbol{a = bx} \cdots\cdots ①$$

とおいて、これをよく眺めてから本題に入ることにしよう.

(1) これは、上記の ① をどう読むか、ということだ.

つまり、これは「**$\boldsymbol{a}$ がどんな整数であっても、常に ① を満たすような整数 $\boldsymbol{b}$ が存在する．そのような $\boldsymbol{b}$ は何か**」と読まなければならない.

そこで、$b = 0$ とすると $a = 0$ となって、「a がどんな整数であっても」という条件に反するので $b \neq 0$ である．そうすると ① は x について解くことができるから

$$x = \frac{a}{b} \longleftarrow \text{これが常に整数！}$$

つまり、「a がどんな整数であっても x が整数でなくてはならない」から $b = 1$ とやりたいが、b は負の数でもよいから $b = \pm 1$ と書かなくてはならない——「**$+1$ と -1 の 2 つ**」がこの場合の答えになる

(2) $\boldsymbol{a = 0}$ のとき ① は

$$0 = bx \cdots\cdots ②$$

だが、「割り切れない」と言っているから「**② を満たす $\boldsymbol{x}$ の整数値が存在しないような整数 $\boldsymbol{b}$ は何か**」と読まなければならない.

仮に $x=0$ とすると ② は $0=b\cdot 0$ で、b が何であっても ① は成立してしまう．したがってそのような整数 b は存在しない．つまり、本問は 「 **ない** 」が正解である．

しかし、この「問いかけ」はイジワルすぎる．そこでチョッと付け加えておくと、大体の場合は a は 0 でないのが常識的であろう．そうすると $b=0$ だと右辺が常に 0 となって等式が成り立たない．だから 最初から $b \neq 0$ としておくべきであろう．そうすれば、もし $a=0$ であっても $x=0$ を選ぶことによって等式を成り立たせることができる．つまり、b は a の約数であり a は b の倍数 (0 倍) であると読みたいところである———この問題は「そうはさせまい」とした入試問題の力作にも見える．

(3) 問題は **負の約数**もシッカリ約数である ということだ．

-1 の約数： $1,\ -1$

0 の約数： 任意の整数

だから、この 2 つの整数に共通の約数、すなわち 1 と 0 の公約数は 1 と -1 で、このうちの最大のものだから、「 **最大公約数は 1** 」である．

(4) 90 と 100 の間の素数は「 **97 ただ 1 つ** 」である．

素数についてはあとで詳しく説明する．

(5) **素数の定義**に注目しておこう———「 1 より大きい整数であって $\cdots\cdots$ 」とあるから 1 は素数ではない．また**合成数**というのは「 正の整数でそれ自身と 1 以外の約数をもつ $\cdots\cdots$ 」というのだから 1 は合成数でもない．素数と合成数は正の整数で考えるので、0 とか負の数は問題外である．また、2 以上の正整数はすべて素数か合成数かのいずれかであり、素数でも合成数でもない正整数は「 **1 のみ** 」である．

出てくる数学用語はどれも普段、何気に使っているコトバである．しかし、どれくらい明快に答えることができただろうか．わかっていると思いながら**「あれっ？」**という思いをしたのではないか．それに、約数、倍数などというと自動的に正の整数と思いがちだが、上記の定義では、ただ整数と言っているだけで正整数とは言っていない．

実は、上記の定義に $\boldsymbol{b \neq 0}$ を付け加えると一般に通用する定義になるのだ．そして、約数、倍数というときは負の整数も 0 も入ってくる のである———ここが何とも悩ましい．

さて、どうだろう．**危うさ**を十分に**満喫**してもらえただろうか．その上で本論に入ることにする．

＜ end. ＞

1.2.1　約数・倍数

1.2.1.1　整除の可能性と一意性

整数の集合 Z は**加法、減法、乗法**について**閉じている**が**除法**すなわち、割り算については**閉じていない**．そこで整数を扱うとき、この除法が特別に関心をひくことになるのである．

ところが除法と言っても、実は 2 通りの扱い方があるのだ——実例で示そう．たとえば 12 を 5 で割る例でみると 2 通りの割り算が考えられるのである．つまり

$12 \div 5 = 2$　余り 2 ····· ①

$12 \div 5 = 2.4$ ····· ②

である——① は整数の枠内のハナシだが ② は整数の枠からハミ出してしまっている．

このとき、① を**整数論的除法** (**整除**) といい、② を**代数的除法**という．ここではもちろん**整除**を問題にするわけである．

整除については次の重要な定理がある．

整除の定理

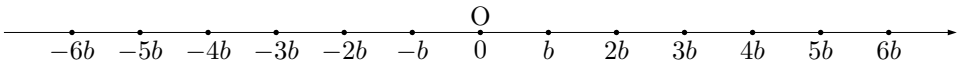
任意の整数 $a,\ b\ (b > 0)$ に対して

$$a = bq + r,\ \text{ただし}\ 0 \leqq r < b$$

となる整数 q, r がただ 1 組存在する．

（**解説**）この定理のキチンとした証明はあとで述べるとして、われわれの目指すところは、まず**この定理が何を主張しているか**を正しく把握することである．

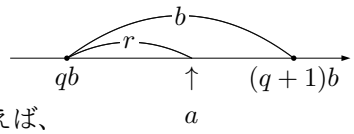
そこで、b に整数をかけたものの全体を数直線上に表してみると



となり、O から左右に遠ざかるにつれて絶対値はいくらでも大きくなる．

そういうわけで

$$qb \leqq a < (q+1)b \cdots\cdots ①$$



となる整数 q が必ず存在する．

しかもただ 1 つだけ存在するはずである．たとえば、$a = -8,\ \ b = 3$ とすれば

$$\underbrace{(-3)\cdot 3}_{-9} \leqq -8 < \underbrace{(-3+1)\cdot 3}_{-6}$$

となって、**1 つ違いの b の整数倍で a をはさむ**カタチにすることができるから、$q = -3$ とすればよいではないか．

そこで ① で a と小さい方の bq との差を r とすれば

$$a - qb = r \qquad \therefore\ \ \boldsymbol{a = qb + r,\ \text{ただし}\ 0 \leqq r < b}$$

が得られることになる．

＜ end. ＞

＜メモ＞

■ $b \leqq 0$ のときはどうするか

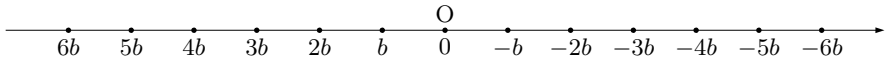
上記では $b > 0$ としたが、$b \leqq 0$ のときはどうすればよいか———一般に、**早わかり**としてナットクするためには $a > 0,\ b > 0$ のときからはじめるとよい．

しかし、そうは言ってもキモチが悪い———どうも $a > 0,\ b > 0$ のときはわかるが負の数が入ってくると混乱するようである．そこで、改めて上記の**整除の定理**は、$b > 0$ として

$$\boldsymbol{a = bq + r,\quad 0 \leqq r < b}$$

だったが、ここで $b \leqq 0$ のときはどう扱えばよいか．もし、$\boldsymbol{b = 0}$ ならば上記で $0 < r < 0$ となり、この定理の意味はない．そこで除数 b が 0 のときは**除外**、つまりは考えないことにする．

問題は $b < 0$ のときだが先に述べた数直線は大小関係をそのままにして考えると目盛りの表示が変わる．つまり



と

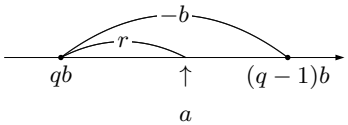
なって、1 **つ違いの** $\boldsymbol{(-b)}$ **の整数倍で** $\boldsymbol{a}$ **をはさむ**カタチにすることができる．

そうすれば本文と同様にして

$$qb \leqq a < (q-1)b$$

そこで $a - qb = r$ とおけば

$$a - qb = r \qquad \therefore\ \ a = qb + r,\ \text{ただし}\ 0 \leqq r < -b$$



この場合をもあわせて表すと**整除の定理**は

$$\boldsymbol{a = bq + r,\quad \text{ただし}\ 0 \leqq r < |b|}$$

としてもよい———ポイントは $\boldsymbol{r}$ **(余り) が負にならないように調整する**のである．

しかし、これも慣れないとマゴつくだろう———例を挙げておくから確認しておくとよい．

(例 1) -25 を 7 で割るには、まず 25 を 7 で割って

$$25 = 7 \times 3 + 4 \qquad \therefore\ \ -25 = -7 \times 3 - 4$$

これを書き変えて、**余り** $\boldsymbol{r}$ **が負にならないように調整する**のである．つまり

$$\begin{aligned} -25 &= 7 \times (-3) - 4 \\ &= 7 \times (-3) - 7 + 3 = \boldsymbol{7 \times (-4) + 3} \end{aligned}$$

だから、$q = -4,\ r = 3$ となる．すなわち、商は -4 で余りは 3 である．

(例 2) -1 を 7 で割る例．

$$\begin{aligned} 1 &= 7 \times 0 + 1 \\ \therefore\ \ -1 &= -7 \times 0 - 1 \\ &= -7 \times 0 - 7 + 6 \\ &= 7(0-1) + 6 = \boldsymbol{7 \times (-1) + 6} \end{aligned}$$

だから、$q = -1,\ r = 6$ である．すなわち、商は -1 で余りは 6 である．

(例 3) 5 を -8 で割る例．

$$5 = (-8) \times 0 + 5$$

で $q = 0,\ r = 5$ である．すなわち、商は 0 で余りは 5 である．

1.2.1.2　約数、倍数の定義

＜1＞ 定義

先に述べた**整除の定理**を思い出してもらいたい．

$$a = bq + r,\ \text{ただし}\ 0 \leqq r < b$$

であった．この等式で、特に $r = 0$ とすると

$$\boldsymbol{a = bq,\ b \neq 0} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

という等式が成り立つ．このとき

1° a は b で**割り切れる**．
2° a は b の**倍数**である．
3° b は a の**約数**である．

などと言うのだが、これらは ① で表された a, b の関係の別表現で、**内容的には全く同じ**ことがらである．

さて、ここで $a = 0$ のときはどうなるか．① で $a = 0$ とおくと

$$0 = bq,\quad b \neq 0 \qquad \therefore\quad q = 0$$

すなわち、条件を満たす q の値は $q = 0$ しかないことがわかる．

したがって上記は

$$0 = b \cdot 0,\quad b \neq 0$$

このとき、b は 0 でない整数なら何でもよいので、「 0 はすべての整数 $(\neq 0)$ で割り切れる 」、あるいは「 0 はすべての整数 $(\neq 0)$ の倍数である 」、あるいは、「 すべての 0 でない整数は 0 の約数である 」ことと同じ意味である．

＜2＞ 約数、倍数に関する基本的な定理

約数、倍数についてのいくつかの性質は、われわれの日常でほとんど自明のことのように使っているが、ここで改めて「 **定理** 」の形で整理しておこう．

約数、倍数についての基本的な定理

(1) $a_1,\ a_2,\ \cdots,\ a_n \in Z$ がすべて m の倍数ならば、任意の整数 $p_1,\ p_2,\ \cdots,\ p_n$ に対して

$$p_1a_1 + p_2a_2 + \cdots + p_na_n$$

もまた m の倍数である．

(2) a が b の倍数 (約数) で、b が c の倍数 (約数) ならば、a は c の倍数 (約数) である．

（解説） (1) は通常、たとえば

「 $a,\ b$ の公約数 g は、任意の整数 $m,\ n$ に対して、常に $ma + nb$ の約数である 」

のような形で用いられる場合が多い．

上記はその拡張版と思ってもらえばよい――改めて証明というほどのことではないが一応やっておこう．まあ、慣れてもらいたい．

a_1〜a_n がすべて m の倍数 (m が a_1〜a_n の公約数) だから、定義より

$$a_k = b_k\ m \quad (\ k = 1,\ 2,\ \cdots,\ n\ ),\quad (\ b_k\text{は整数}\ )$$

とおくことができる．すなわち

$$\sum_{k=1}^{n} p_k a_k = m \sum_{k=1}^{n} p_k b_k$$

で、$\displaystyle\sum_{k=1}^{n} p_k b_k$ は整数 (整数の集合 Z は積と和について閉じている) であるから、$\displaystyle\sum_{k=1}^{n} p_k a_k$ は m の倍数である．

(2) これも当たり前のことだが、まあ、やっておく．

まず倍数である場合について考察する．

$$\left.\begin{array}{l} a\text{ が }b\text{ の倍数} \longrightarrow a = bm\ (m\text{ は整数}) \\ b\text{ が }c\text{ の倍数} \longrightarrow b = cn\ (n\text{ は整数}) \end{array}\right\} \quad \therefore\ \ a = cmn$$

つまり、mn は整数だから、a は c の倍数である．

次に約数である場合は

$$\left.\begin{array}{l} a\text{ が }b\text{ の約数} \longrightarrow b = al\ (l\text{ は整数}) \\ b\text{ が }c\text{ の約数} \longrightarrow c = bk\ (k\text{ は整数}) \end{array}\right\} \quad \therefore\ \ c = alk$$

つまり、lk は整数だから、a は c の約数である．

＜ end. ＞

1.2.2　最大公約数・最小公倍数

1.2.2.1　定義

いくつかの整数 $a,\ b,\ \cdots\cdots$ に共通な約数をこれらの数の**公約数**という．たとえば、12 と -18 の公約数を考えてみよう．

$$\begin{array}{ll} 12\text{ の約数} & :\ \pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12 \\ -18\text{ の約数} & :\ \pm 1,\ \pm 2,\ \pm 3,\ \pm 6,\ \pm 9,\ \pm 18 \end{array}$$

これらをよく睨んで、12 と -18 の公約数は $\pm 1,\ \pm 2,\ \pm 3,\ \pm 6$ である．

一般に $a\ (\neq 0)$ の約数 g というとき

$$-|a| \leqq g \leqq |a| \ \longleftarrow\ a \text{ は与えられた整数！}$$

であるから、その個数は有限個である．しかし、$a = 0$ のときは、0 の約数はすべての整数 $(\neq 0)$ だからこれは無限個である．そこで、整数 $a,\ b,\ \cdots\cdots$ の中に 0 でないものが少なくとも 1 つあれば、それらの公約数は有限個だから、その中には最大のものがある．それを整数 $a,\ b,\ \cdots\cdots$ の**最大公約数**という．

一方、いくつかの整数 $a,\ b,\ \cdots\cdots$ に共通な倍数をこれらの数の**公倍数**という．たとえば、-4 と 6 の倍数は

$$\begin{array}{ll} -4\text{ の倍数} & :\ 0,\ \pm 4,\ \pm 8,\ \pm 12,\ \cdots\cdots \\ 6\text{ の倍数} & :\ 0,\ \pm 6,\ \pm 12,\ \pm 18,\ \cdots\cdots \end{array}$$

だが、これらは無数にある．

この倍数のうち、0 と負の整数を除くと

$$\begin{array}{ll} -4\text{ の倍数} & :\ 4,\ 8,\ 12,\ 16,\ \cdots\cdots \\ 6\text{ の倍数} & :\ 6,\ 12,\ 18,\ ,24\cdots\cdots \end{array}$$

となり、これらから共通のものをとりだすと、**下に有界**である自然数の集合が得られるから、その要素の中には最小のものがあるはずである——上記の場合は 12 がそれにあたる．一般に整数 $a,\ b,\ \cdots\cdots$ の公倍数のうち、正で最小のものを整数 $a,\ b,\ \cdots\cdots$ の**最小公倍数**という．

(注)　「 **G.C.M.** 」と「 **L.C.M.** 」

”**最大公約数**”というコトバの表現は長ったらしくて、読んでも書いてもわずらわしい．そこで最大公約数のことを **G.C.M.** と略記することもある．これは Gratest Common Measure の頭文字をとったものである．以下、適宜に用いることにする．

”**最小公倍数**”についても同様で、**L.C.M.** と略記する．これは Least Common Multiple の頭文字をとったものである．

(注) ＜ end. ＞

1.2.2.2 「 最大公約数 」、「 最小公倍数 」に関する定理

$ab \neq 0$ で、しかも $a,\ b$ の「 G.C.M. 」が 1 であるとき、a と b は**互いに素**であるという．ただしこの場合、当然のことながら $a \in Z,\ b \in Z$ である．

このとき、これを**素数**と混同しないよう注意しなければならない．たとえば、12 と 25 は互いに素であるがいずれも素数ではない———素数とその扱い方についてはあとで詳しく説明する

ここでのテーマは、「 G.C.M. 」、「 L.C.M. 」だが、いくつか**無視できない**定理があるので、以下に示しておく———解説を追いながら、その扱い方に慣れてもらいたい．

定理 1

(1) $a,\ b,\ \cdots(\in Z)$ の公倍数 x は、それらの「 最小公倍数 」l の倍数である.

(2) $a,\ b,\ \cdots(\in Z)$ の公約数 x は、それらの「 最大公約数 」d の約数である.

(**解説**) 実は、この (2) は (1) を用いて証明することになる.

したがって、この **(1) と (2) はセットで理解**しておくのがよい かと思う.

(1) 公倍数のうち、特に「 L.C.M. 」に注目するのは、この定理ゆえのことである.

つまり、「 L.C.M. 」が求まればすべての公倍数はその倍数として確定するのだからありがたい——証明は次のようにやる.

x を、上記の「 L.C.M. 」l で割った商を q、余りを r とすると

$$\boldsymbol{x = lq + r,\ \ 0 \leqq r < l} \longleftarrow \textbf{整除の定理！}$$

$$\therefore\ \ r = x - lq$$

ここで、$x,\ l$ は $a,\ b,\ \cdots\cdots$ の公倍数であるから $x - lq\ (= r)$ も $a,\ b,\ \cdots\cdots$ の公倍数である.

そこで、$r \neq 0$ とすると $0 < r < l$ となり、r が l より小さい公倍数ということになって、l が「 L.C.M. 」であるという条件に矛盾する.

したがって $r = 0$、すなわち $\boldsymbol{x = lq}$ がいえて x が l の倍数であることがわかる.

(2) これも**おいしいハナシ**だ.

つまり、「 G.C.M. 」d を求めることができれば、その約数としてすべての公約数を求めることができる ということだ. しかし困ったことに、この定理の証明は**ちょっと難しい**——まあ、ソロソロとやってみるか.

もし、x が d の約数ならば、x と d の「 L.C.M. 」は d である. 逆に x と d の「 L.C.M. 」が d ならば x が d の約数であることは明らかだ.

そういうことなら、x と d の「 L.C.M. 」を l とするとき、$l = d$ がいえればよいことにならないか——「 $l \geqq d$, かつ $l \leqq d$ 」をいえばよい.

まず、l は x と d の「 L.C.M. 」だから

$$\boldsymbol{d \leqq l} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

である. これは問題ない——あとは $d \geqq l$ をいう.

そこで、ハナシをもとにもどすと a は x の倍数であり、また「 G.C.M. 」d の倍数でもあるから (1) によって l の倍数である.

同様にして $b,\ \cdots$ も l の倍数である. すなわち、l は $a,\ b,\ \cdots$ の公約数なのである. つまり、d は $a,\ b,\ \cdots$ の「 G.C.M. 」だから

$$\boldsymbol{d \geqq l} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ②$$

①, ② から $\boldsymbol{l = d}$ となり、したがって x は d の約数であることがわかる.

＜ end. ＞

定理 2

2 つの正整数 a, b の「 G.C.M 」を d、「 L.C.M. 」を l とし

$$a = da', \quad b = db' \quad (a',\ b' \text{は整数})$$

とおくと次の結果が得られる．すなわち

(1) $a',\ b'$ は互いに素である．
(2) $l = da'b'$
(3) $ab = dl$

(**解説**) この定理は 2 つの正整数について成り立つハナシであって、3 つ以上の整数に勝手に拡張してはならない——ウッカリやりそうなので特に注意しておく．

(1) $a',\ b'$ が互いに素というのは、$a',\ b'$ の「 G.C.M. 」が 1 ということだから、証明の方法としては $a',\ b'$ の「 G.C.M. 」を d' として、$d' > 1$ では不合理が起こることをいえばよい．具体的には

$$a' = d'a'', \quad b' = d'b'' \quad (a'', b'' \in Z)$$

とおくと

$$a = a'' \cdot dd', \qquad b = b'' \cdot dd'$$

となり、dd' は $a,\ b$ の公約数である．そして、$d' > 1$ ならば $dd' > d$ となり、$a,\ b$ には「 G.C.M. 」d より大きい公約数 dd' があることになって不合理である．

よって $d' = 1$、すなわち a' と b' とが互いに素であることが示された．

(2) $da'b' = m$ とおくと、$m = ab' = a'b$ であるから、m は $a,\ b$ の公倍数で、前掲の「 **定理 1** (1) 」により m は「 L.C.M. 」l の倍数である．

そこで

$$m = lk \quad (k \in Z) \quad (= ab' = a'b\ ) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

とおくと、l は $a,\ b$ の倍数だから

$$l = aa'' = bb'' \quad (a'',\ b'' \in Z) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ②$$

とおくことができる．

そこで ② を ① に入れて、それぞれの関係を表すと

$$aa''k = ab', \quad bb''k = a'b \qquad \therefore \quad a' = b''k, \quad b' = a''k$$

だが、ここで (1) より $a',\ b'$ が互いに素であるから $k = 1$ でなければならない．

すなわち

$$m = l \qquad \therefore \quad l = da'b'$$

である．

(3) (2) の結果を利用する．

すなわち

$$ab = a'd \cdot b'd = d \cdot da'b' = dl$$

である．

＜ end. ＞

定理 3

(1) ab が c で割り切れ、b と c が互いに素であるときは、a は c で割り切れる.

(2) c が $a,\ b$ で割り切れ、かつ a と b が互いに素であれば、c は ab で割り切れる.

(**解説**) ちょっと見に (1) (2) とも当たり前である.

”何をいまさら”と思うかも知れないが、しばらくガマンして付き合ってもらいたい. 実際、こういうことを数式でキチンと示すのは難しい———以下にやっておく.

(1) 前掲の「 **定理 2 (3)** 」を用いて証明する.

$b,\ c$ の「 G.C.M. 」を d、「 L.C.M. 」を l とすると

$$bc = dl$$

だが、$b,\ c$ は互いに素であるから $d = 1$、すなわち $bc = l$ である.

一方、条件から ab は c の倍数であり、また当然 b の倍数でもあるから ab は $b,\ c$ の公倍数である. したがって「 **定理 1** (1) 」により ab は $l\ (= ab)$ の倍数である.

ゆえに

$$ab = bck\ (k \in Z) \qquad \therefore\quad a = ck$$

よって、a は c で割り切れる.

(2) 条件から c は a で割り切れるから、$c = c'a$ とおくと、これは b でも割り切れる.

ところが、a と b は互いに素であるから (1) により c' は b で割り切れる. すなわち、$c' = c''b$ と置くことができるから

$$c = c'a = c''ab\ \ (c',\ c'' \in Z)$$

となり、c は ab で割り切れる.

＜ end. ＞

(**注 1**)「 **定理 3 (2)** 」についての補足

つまり、c が a で割り切れ、かつ b で割り切れたとしても、c が ab で割り切れるとは限らないのである. たとえば、上記の $a,\ b,\ c$ が

$$c = 12,\quad a = 4,\quad b = 6$$

などのとき、12 は 4 でも 6 でも割り切れるが、その積 24 $(= ab)$ では割り切れない.

それは、4 と 6 が互いに素でないことによるのである.「 **定理 3** (2) 」の中で $\boldsymbol{a}$ **と** $\boldsymbol{b}$ **が互いに素**という条件がきわめて重要な意味をもっているのである. まずは、このことをシッカリと確認しておいてもらいたい.

(**注 2**) 「 **定理 3 (2)** 」の拡張

この (2) を拡張すると、c が $a,\ b$ の公倍数であれば、c は $a,\ b$ の「 L.C.M. 」で割り切れる、となって前掲の「 **定理 1** (1) 」になる.

特に $a,\ b$ が互いに素であるときは「 **定理 2** 」によって $a,\ b$ の「 L.C.M. 」は ab となり、これは「 **定理 1** (1) 」の特別な場合であることがわかる.

(**注**) ＜ end. ＞

＜メモ＞

■ 最大公約数と最小公倍数

とにかく 1 つ 2 つやってみないことにはハナシにならない．とりあえずは、確認用の問題だ．

＜ 例 **1** ＞

(1) 次の各組の最大公約数と最小公倍数を求めよ．

(i) (5040, 8316)　　(ii) (899, 1073, 2523)

(2) 2787, 3579, 4635 のいずれを割っても 15 余る数の中で、最大のものを求めよ．

(解) (1) まずは、**素因数分解**ができるか．

(i) 2 数を分解すると

$$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7, \qquad 8316 = 2^2 \cdot 3^3 \cdot 7 \cdot 11$$

$$\therefore \quad \text{G.C.M.} = 2^2 \cdot 3^2 \cdot 7 = 252, \qquad \text{L.C.M.} = 2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 = 166320$$

あるいは、「 G.C.M. 」が求まったところで、前掲の「 **定理 2 (3)** 」を用いる．

$$\text{L.C.M.} = \frac{ab}{d} = \frac{5040 \times 8316}{252}$$

を計算してもよい———公式を覚えるだけでなく、生きた知識として、まず慣れること！

(ii) (i) と同様に 3 数を分解する．

$$899 = 29 \cdot 31, \qquad 1073 = 29 \cdot 37, \qquad 2523 = 3 \cdot 29^2$$

$$\therefore \quad \text{G.C.M.} = 29, \qquad \text{L.C.M.} = 3 \cdot 29^2 \cdot 31 \cdot 37 = 2893881$$

だが、数値が大きくて分解しにくい———**ユークリッドの互除法** (後述) がよさそうだ．

(2) 3 数を x で割って、いずれも余りが 15 であるから、3 数から先に 15 を引いておけば、いずれも x で割り切れるということになる．

$$2787 - 15 = 2772, \qquad 3579 - 15 = 3564, \qquad 4635 - 15 = 4620$$

したがって、x は 2772, 3564, 4620 の公約数で、そのうち最大のものというのだから、この 3 数の「 G.C.M. 」を求めればよい．

ここで

$$2772 = 2^2 \cdot 3^2 \cdot 7 \cdot 11, \qquad 3564 = 2^2 \cdot 3^4 \cdot 11, \qquad 4620 = 2^2 \cdot 3 \cdot 7 \cdot 11$$

であるから、求める数は

$$2^2 \cdot 3 \cdot 11 = 132$$

で、意外に簡単にいった．しかし、**互除法**を用いて機械的にやるなら、まず 2 つずつセットにして、それぞれの G.C.M. を求め、さらにその G.C.M. を求めてもよい———各自で研究のこと．

＜ end. ＞

＜例 **2**＞

次の条件に適する 2 つの自然数を求めよ．

(1) 和が 54 で、最大公約数が 6

(2) 積が 864 で、最小公倍数が 144

(3) 3 桁の自然数で、最大公約数が 29、最小公倍数が 4147

(解) 2 数の**和**、**積**、そして**最大公約数**、**最小公倍数**の混合問題である．

整数 $a,\ b$ の「 G.C.M. 」を g とするとき

$$a = a'g,\quad b = b'g \ \longleftarrow\ a', b' \text{は互いに素！}$$

だが、条件の**和**とか**積**とか「 **L.C.M.** 」から得られる $a' + b'$ の例を 1 つ、$a'b'$ の例を 2 つ用意した．いずれも、それぞれの**不定方程式**を単独に解くことになる――やってみてもらいたい．

(1) 最大公約数が 6 だから

$$a = 6a',\quad b = 6b' \ \longleftarrow\ a', b' \text{は互いに素！}$$

条件から

$$a + b = 6a' + 6b' = 6(a' + b') = 54 \qquad \therefore\ \boldsymbol{a' + b' = 9} \ \longleftarrow\ \text{不定方程式！}$$

ゆえに、これを満たす自然数は

a'	1	2	4
b'	8	7	5

$\therefore$

a	6	12	24
b	48	42	30

で、求める 2 数は $(6,\ 48)$, $(12,\ 42)$, $(24,\ 30)$ の 3 組である．

(2) 2 数 $a,\ b$ の「 G.C.M. 」を g とすると $\boldsymbol{a = ga',\ \ b = gb'}$ **($a',\ b'$は互いに素)** までは同じでよかろう．そうすると条件は

$$\begin{cases} ab = (ga')(gb') = g^2a'b' = 864 \\ \text{「 L.C.M. 」} = ga'b' = 144 \end{cases} \qquad \therefore\ g = 6 \qquad \therefore\ \boldsymbol{a'b' = 24} \ \longleftarrow\ \text{不定方程式！}$$

ここで、24 を互いに素である 2 数 $a' < b'$ の積に分解すると

a'	1	3
b'	24	8

$\therefore$

a	6	18
b	144	48

すなわち、求める 2 数は $(6,\ 144)$, $(18,\ 48)$ の 2 組である．

(3) これも、2 数 $a,\ b$ の「 G.C.M. 」は $g = 29$ で、$\boldsymbol{a = 29a',\ \ b = 29b'}$ **($a',\ b'$は互いに素)** となる．そうすると条件は

$$\text{「 L.C.M. 」} = 29a'b' = 4147 \qquad \therefore\ \boldsymbol{a'b' = 143 = 11 \cdot 13} \ \longleftarrow\ \text{不定方程式！}$$

で、$(a',\ b')$ の組は

a'	1	11
b'	143	13

であるが、条件に $a',\ b'$ に 29 をかけて得られる $a,\ b$ が 3 桁という制限があるので、求める整数の組は $(a',\ b') = (11,\ 13)$ に対する $(a,\ b) = (319,\ 377)$ となる．

＜ end. ＞

■ $\boldsymbol{a+b}$ と $\boldsymbol{ab}$——「 隠れインフラ 」とその整備 ！

これは説明しないとわからないかも知れないが、これをクリアしておかないとちょっとしたときに、何とも不便なことになってしまう．以下、ポイントを「 **定理** 」としてまとめておく．

定理

> $\boldsymbol{a}$, $\boldsymbol{b}$ が互いに素のとき、$\boldsymbol{a \pm b}$ と $\boldsymbol{ab}$ もまた互いに素である．

(解説) ちょっと見には、ごく当たり前なことだが、改めてマジメに考えると、一瞬「 えっ 」と思わないか———これがないと、何とも具合が悪いときがあるのです．

証明は、$a+b$ と $a-b$ の場合はほぼ同じだから、$a+b$ の場合だけをやっておく．つまり

「 $\boldsymbol{a}$, $\boldsymbol{b}$ が互いに素 」のとき、「 $\boldsymbol{a+b}$ と $\boldsymbol{ab}$ もまた互いに素 」である．

ということだ———**背理法**で証明する．

a, b が互いに素であるとき、ab と $a+b$ が互いに素でないと仮定 する．そして、そのときの公約数の 1 つを p (>1) とすると、$a+b$ は p で割り切れ、ab も p で割り切れる．

これは、a か b かのどちらかが p で割り切れるということだから、仮に a が p で割り切れるとしておこう．そうすると

$$\begin{cases} a+b=kp \\ a=lp \end{cases} \qquad \therefore\ \ b=kp-a=p(k-l) \ \longleftarrow\ \boldsymbol{b}\text{ は }\boldsymbol{p}\text{ の倍数！}$$

これは、最初の条件「 a, b が互いに素 」に反して**不合理**である———これは、b が p で割り切れるとしても同じことは説明するまでもない．したがって、上記が証明された．

＜ end. ＞

さて、準備のできたところで、次の問題をやってみてもらいたい．

＜ 例 1 ＞

> 和が 1092 で、最小公倍数が 3528 である 2 数を求めよ．

(解) 2 数 a, b の「 G.C.M. 」を g とすると $\boldsymbol{a=ga'}$, $\boldsymbol{b=gb'}$ $\boldsymbol{(a', b'}$**は互いに素)** だから

$$a+b=ga'+gb'=g(a'+b')=1092\ (=2^2\cdot 3\cdot 7\cdot 13)\ \cdots\cdots\cdots\cdots\cdots ①$$

$$「\ \text{L.C.M.}\ 」=ga'b'=3528\ (=2^3\cdot 3^2\cdot 7^2)\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ②$$

ここで、**上記の定理**である．つまり、「 $\boldsymbol{a'}$ と $\boldsymbol{b'}$ が互いに素であるから $\boldsymbol{a'+b'}$ と $\boldsymbol{a'b'}$ も互いに素 」である ことがいえる．結果、g は 1092 と 3528 の「 G.C.M. 」となる．

したがって ① ② から

$$g=2^2\cdot 3\cdot 7=84$$

が得られるから、これを ① ② に入れて

$$\boldsymbol{a'+b'=13}, \quad \boldsymbol{a'b'=2\cdot 3\cdot 7=42}$$

ここで、**解と係数の関係**を使えば a', b' は次の 2 次方程式の解である．すなわち

$$t^2-13t+42=(t-6)(t-7)=0 \qquad \therefore\ \ t=6,\ 7\ \longleftarrow\ \boldsymbol{a', b'}\text{ は互いに素を満たす！}$$

ゆえに

$$a=84\times 6=504, \quad b=84\times 7=588$$

したがって、求める 2 数は (504, 588) である．

＜ end. ＞

1.2.2.3　ユークリッドの互除法

＜1＞ 互除法とは何か

最大公約数を求めるには、小学生のときからやってきたように、それぞれの整数を素数の積に分解し、その構成を眺めて公約数のうちの最も大きいものを確定するのが最も一般的な方法であると言ってよいだろう——素朴ではあるが、前掲の「 **定理 2** 」を根拠とした、誰もが認める方法である.

ユークリッドの互除法も 2 つの整数の**最大公約数**を求める方法論の 1 つであるが、ちょっとハイテクというか、まあ、先に述べた**整除の定理**を利用するもので敷居が高いといえばいえる内容ではある.

しかし、だからといってどちらが優れているとかいうことではなくて、それぞれ存在理由があり、使い勝手の問題もあるので無視して通過することもできない.

たとえば、144 と 360 の「 G.C.M. 」を求めるにはどうするか.

$$144 = 2^4 \cdot 3^2 \qquad 360 = 2^3 \cdot 3^2 \cdot 5$$

と、それぞれの整数を**素因数分解**する——素因数分解についてはあとで詳しく説明する.

そこで 2 つの整数の構成が見えるから前掲の「 **定理 2** 」により

$$\text{G.C.M.}: \quad 2^3 \cdot 3^2 = 72$$
$$\text{L.C.M.}: \quad 2^4 \cdot 3^2 \cdot 5 = 720$$

である——さして難しいハナシではない.

ところが、11951 と 11063 などの「 G.C.M. 」を求めるとなると、そう簡単には行かない. ちょっと苦しいが、頑張って**素因数分解**してみると

$$11951 = 17 \cdot 19 \cdot 37 \qquad 11063 = 13 \cdot 23 \cdot 37$$

となる. しかし、素数の数値が大きいのであまりラクではない——**ユークリッドの互除法**はこういうときに「 **威力を発揮する** 」のである. 以下、簡単に**互除法**と略記する.

互除法については、その**基本原理**も説明しなければならないが、とりあえず**やり方**の説明から入ることにする.

上記の 11951 と 11063 などの「 G.C.M. 」を求める例でいうと

(1) 11951 を 11063 で割って余り r_1を得る.
(2) 除数であった 11063 を余りであった r_1で割って余り r_2を得る.
(3) 除数であった r_1を余りであった r_2で割って余り r_3を得る.

.....
.....
.....

と、交互に割り算を繰り返していくと、最大公約数があるなら最後には割り切れる.

このとき、**最後に割り切った数**が求める最大公約数である——と、いわれても何のことやらわからないだろうから実例でやって見せよう.

以下に実際の計算を示しておくが、何をやっているのかを考えながら計算を追って結果を確認し、できればソコソコ感動してもらえると筆者としてはとてもうれしい.

以下、計算を追って確認してもらいたい.

$$
\begin{array}{r}
1 \\
11063\,\overline{)\,11951} \\
\underline{11063} \\
888
\end{array}
\qquad
\begin{array}{r}
12 \\
888\,\overline{)\,11063} \\
\underline{888} \\
2183 \\
\underline{1776} \\
407
\end{array}
\qquad
\begin{array}{r}
2 \\
407\,\overline{)\,888} \\
\underline{814} \\
74
\end{array}
\qquad
\begin{array}{r}
5 \\
74\,\overline{)\,407} \\
\underline{370} \\
37
\end{array}
\qquad
\begin{array}{r}
2 \\
37\,\overline{)\,74} \\
\underline{74} \\
0
\end{array}
$$

(1) (2) (3) (4) (5)

まあ、ざっとこんなものだが、**最右端の計算**を見てもらいたい．その前の段階 (右から 2 番目)、つまり (4) の計算で除数であった 74 を余りであった 37 で割っている．

しかもシッカリ**割り切れている**ではないか．このとき、11951 と 11063 の最大公約数が、その最後に割り切った数 37 である というのである．

これは相当に**おいしいハナシ**なのだ——それは、もしこの方法が信頼できるなら、大きい数値どうしの最大公約数を求める場合、やればヤッカイになるであろう素因数分解を避けて通ることができるではないか．

これはユークリッドの**幾何学原本**にでてくるそうだが、恥ずかしながら筆者はまだ確認していない．ともあれ、それが**ユークリッドの互除法**という名前の所以であろう．

ユークリッド (紀元前 365 年？〜紀元前 275 年？) といえば、プトレマイオス 1 世治世下、エジプトのアレクサンドリアで活躍した数学者といわれている——はるか霧の彼方の、さらにその先の話である．スゴイ人がいたものだ．それを、こともあろうに 21 世紀の今日、私たちが大マジメに勉強するのも不思議なハナシではある．

ちなみに、パソコンは「 互除法 (次に述べる) はできるが素因数分解はできない 」と誰かに聞いたような気がする．人力 (じんりき) も捨てたものではない．

(注) 互除法を表現する形式

やり方は本文に説明したが、さてそれをどう書いたものか．上記の 11951 と 11063 を例にして説明しておこう．一般には次のように書くようである．

ただし、左右の矢印をつけた説明は、読者が混乱しないように筆者がつけたものだから、実際の計算では書く必要はない———やりながらわかっていればそれでよい．

11951 を 11063 で割る ⟶ 1	11951	11063	12 ⟵ 11063 を 888 で割る
	11063	10656	
888 を 407 で割る ⟶ 2	888	407	5 ⟵ 407 を 74 で割る
	814	370	
74 を 37 で割る ⟶ 2	74	37	
	74		
	0		

まあ、こういうことになるが、筆者の個人的なカンジでいうと、左右に現れる数値が 1 桁のときは何となくキモチがよいが、この例のように 12 など、2 桁以上になると、別の計算用紙で計算して数値を決めておかないと、「 いきなり 」では書きにくい．

それに、何だか覚えにくいような気がする．筆者も本稿を書きながら「 昔やったんだが、どうだったっけ 」と思ったりしたほどである．そこで、改めて考えてみた．

そうすると、どうやら本文の (1) から (5) に述べた計算を右から書くとよさそうなことが見えてきた．つまり、右から書いておいて、そのまま「 ガチャン 」と接続する．そうすれば「 いつもの割り算の形式通り 」にやればよいから、まず間違えたり忘れたりすることはない だろう．

以下は、それを簡略に「 表 」で表したものであるが、念のため、通常の割り算の形式になっている部分の 1 セット分にアミをかけておいた———各ブロックにこの形式の割り算を行っているわけである．

上記の計算と対応させながらその経緯を確認しておくとよい．

	(5)	(4)	(3)	(2)	(1)
	2	5	2	12	1
37	74	407	888	11063	11951
	74	370	814	888	11063
	0	37	74	2183	888
				1776	
				407	

(注) ＜ end. ＞

＜2＞ 互除法を保証する定理

さて、それはともかく、われわれは上記の計算から何をつかめばよいか．それはひたすら**次の定理**に集約されるのである——ちょっと頑張ってみる価値はありそうだ．

互除法を保証する定理

$a,\ b,\ q,\ r\ \in Z$ として

$$a = bq + r \quad 0 \leqq r < |b| \cdots\cdots (*)$$

のとき、$a,\ b$ の公約数全体の集合 P と $b,\ r$ の公約数全体の集合 Q とは一致する．

(**解説**) いきなり、「 集合が一致する 」という表現はキツイかも知れない——そのために、(**注**) として**別の説明**も用意しておいた．

さて、集合の一致、すなわち

$$\boldsymbol{P = Q \iff P \subseteqq Q,\ \text{かつ}\ P \supseteqq Q}$$

$P \subseteqq Q,\ P \supseteqq Q$ のどちらから始めてもよいが、上記の $(*)$ の右辺のカタチを見ると $P \supseteqq Q$ から始めるのが自然のように見える．

(i) $\boldsymbol{Q \subseteqq P}$ であること．

いま、<u>Q の任意の要素を d とおくと</u>、$\boldsymbol{b = db',\ \ r = dr'}$ $(b',\ r'\ \in Z)$ であるから

$$\begin{aligned} a &= bq + r \\ &= db'q + dr' = d(b'q + r') \ \longleftarrow\ \boldsymbol{a}\ \text{は}\ \boldsymbol{d}\ \text{の倍数！} \end{aligned}$$

これより、d は $a,\ b$ の公約数であることがわかる．すなわち

$$d \in P \quad \therefore\ \boldsymbol{Q \subseteqq P} \cdots\cdots ①$$

(ii) $\boldsymbol{P \subseteqq Q}$ であること．

<u>P の任意の要素を d' とおくと</u>、$\boldsymbol{a = d'a',\ \ b = d'b'}$ $(a',\ b'\ \in Z)$ であるから、$(*)$ を変形して

$$\begin{aligned} r &= a - bq \\ &= d'a' - d'b'q = d'(a' - b'q) \ \longleftarrow\ \boldsymbol{r}\ \text{は}\ \boldsymbol{d'}\ \text{の倍数！} \end{aligned}$$

これより、d' は $b,\ r$ の公約数、すなわち

$$d' \in Q \quad \therefore\ \boldsymbol{P \subseteqq Q} \cdots\cdots ②$$

結局、①② が成り立つので $\boldsymbol{P = Q}$ であることが示された．

かくして、<u>割られる数 a と割る数 b との最大公約数が割った数 b と余り r の最大公約数に次々に一致し、先に述べた例のように、ついには割り切れる</u>．

そして、<u>結局、a と b との最大公約数が、割った数 37 と余り 0 との最大公約数 37 に一致する</u> ことになるわけである．

＜ end. ＞

(注) 互除法を保証する定理 (簡易版)

上記の証明は大上段にかまえて、**集合の包含関係**を用いたので、ちょっと大げさに見えるキライがある．とはいえ、これはこれで重要な視点だから、必ずマスターしておかなければならない．

しかし、もう少し**カジュアルな表現**の方が親しみ易くて好ましい———要は次のように言い換えても同じことなのだ．すなわち

互除法を保証する定理 (簡易版)

2 つの正整数 $a,\ b$ があって、a を b で割った余りを r とすると、$a,\ b$ の「 G.C.M. 」は $b,\ r$ の「 G.C.M. 」と一致する．

(証明) $a,\ b$ の「 G.C.M. 」を g として

$$\boldsymbol{a = ga',\ \ b = gb'\ \ \ (a',\ b'\ \in Z)}$$

とおくと $a = bq + r$ だから

$$\begin{aligned} r &= a - bq \\ &= ga' - gb' \cdot q = g(a' - b'q) \ \longleftarrow\ g \text{ は } r \text{ の約数！} \end{aligned}$$

すなわち、g は $b,\ r$ の公約数である．そこで、$b,\ r$ の「 G.C.M. 」を g' とすると

$$\boldsymbol{g \leqq g'} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

また、$b = g'b'',\ \ r = g'r'$ とおくと

$$\begin{aligned} a &= bq + r \\ &= g'b''q + g'r' = g'(b''q + r') \end{aligned}$$

すなわち、g' は $a,\ b$ の公約数である．

ここで、$a,\ b$ の「 G.C.M. 」が g であるから

$$\boldsymbol{g \geqq g'} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ②$$

となり、結局 ①② から $\boldsymbol{g = g'}$ であることがわかる———この方がスッキリしていてよいと思うのは私の好みだろうか．

＜ end. ＞

(注) ＜ end. ＞

＜メモ＞

■ 改めて、「 整除の定理 」とその応用

互除法のやり方、書き方についてはかなり詳しく述べたから、それはもうヨシとして、ここではその「 互除法の基本原理 」そのものでもある「 整除の定理 」と「 その応用 」について改めて考えてみる――なかなか重宝な使い方があるのです.

$a,\ b,\ q,\ r\ \in Z$ として

$$\boldsymbol{a = bq + r} \quad 0 \leqq r < |b| \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

をながめてみてもらいたい．ここでハナシを簡単にするために

$$a = a'p,\quad 0 < a' < b$$

として説明する．いま仮に

$$b = a' + c \longleftarrow \boldsymbol{c}\text{ を }\boldsymbol{b}\text{ より小さい値にとることができる！}$$

と表せたとすると、これを $(*)$ に入れると

$$\begin{aligned} a &= bq + r \\ &= (a' + c)q + r = a'q + cq + r \\ \therefore\ & \boldsymbol{a'(p - q) = cq + r} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (**) \end{aligned}$$

まず、$(*)$ と $(**)$ の右辺で何が起こっているか――「 q の係数 b が、より小さい値 c に置き換えられている 」ではないか．しかも、$(**)$ の左辺は a' の倍数になっている．

だから、これを繰り返していけば q の係数の縛りをきつくしていくことができる．そして、これは**不定方程式**を解くときなども**きわめて有効**であるから、トウゼン知っていた方がよい．

しかし、そうは言ってもピンとはこないだろうから、実例で説明する．

＜ 例 ＞

12 で割ると 5 余り、17 で割ると 6 余るような数の中で最小のものを求めよ．

(解) 12 で割ると 5 余り、17 で割ると 6 余る自然数を N とし、12, 17 で割った商をそれぞれ $p,\ q$ とすると

$$N = 12p + 5 = 17q + 6 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

で、これは $p,\ q$ についての**不定方程式**だが、その一般的な扱い方はあとで解説するので、ここでは「 **約数、倍数の問題** 」として考察を進めることにする．

① を変形すると

$$12p = 17q + 1 = 12q + 5q + 1 \qquad \therefore\ \ 12(p - q) = 5q + 1$$

これより、右辺の $5q + 1$ は 12 の倍数だから、これを改めて $12r$ とおく と

$$\boldsymbol{5q + 1 = 12r} = 10r + 2r \qquad \therefore\ \ \boldsymbol{5(q - 2r) = 2r - 1}$$

ここも同様に、$2r - 1$ が 5 の倍数だから、これを $5s$ とおく と

$$\boldsymbol{2r - 1 = 5s} = 4s + s \qquad \therefore\ \ \boldsymbol{2(r - 2s) = s + 1}$$

これより $s + 1$ が 2 の倍数で、これを $2n$ とおく と

$$\boldsymbol{s + 1 = 2n} \qquad \therefore\ \ s = 2n - 1$$

となる――あとは $r,\ q,\ p$ と順次たどって N を求める．

まず r を求めると

$$2r - 1 = 5s = 5(2n - 1) \qquad \therefore\ \ 2r = 10n - 4 \qquad \therefore\ \ r = 5n - 2$$

これを用いて q を求めると

$$5q + 1 = 12r = 12(5n - 2) \qquad \therefore\ \ 5q = 60n - 25 \qquad \therefore\ \ q = 12n - 5$$

① では q が求まれば N が求まるから

$$\begin{aligned} N &= 17q + 6 \\ &= 17 \cdot (12n - 5) + 6 = 204n - 79 \end{aligned}$$

これが正で最小になるのは $n = 1$ のときで、その最小値は

$$204 \cdot 1 - 79 = 125$$

である.

★ 数列として見る

12 で割ると 5 余る自然数、17 で割ると 6 余る自然数を小さい順に並べて数列 A, B を作ってみると

$$A \ : \ 5,\ 17,\ 29,\ 41,\ 53,\ \cdots\cdots\cdots\cdots\cdots$$
$$B \ : \ 6,\ 23,\ 40,\ 57,\ 74,\ \cdots\cdots\cdots\cdots\cdots$$

だが、この 2 つの等差数列で「 最初に出てくる共通項 」が求める数である.

そういうことなら、この数列を並べて調べればよいわけだが、かなり多くの項をとらないと、その共通項にたどりつかない.

こういう場合は、共通項のみで作る等差数列は 12 と 17 の**最小公倍数** 204 がその公差になることを知っていれば、答えは簡単に求めることができる.

この例でいえば、共通項の等差数列は

$$a_n = 125 + (n - 1) \cdot 204 \quad \longleftarrow \text{ 一般項！}$$

である———いろいろあるものだ.

＜ end. ＞

1.2.3　剰余類

1.2.3.1　剰余系と類別

右は 2010 年 12 月のカレンダーである．よく眺めてもらいたい———この表の特徴は何か．たとえば、火曜日の数 7, 14, 21, 28 はすべて 7 で割り切れる．

つまり

火曜日の数：　7 で割り切れる．
水曜日の数：　7 で割ると 1 余る．
木曜日の数：　7 で割ると 2 余る．
金曜日の数：　7 で割ると 3 余る．
土曜日の数：　7 で割ると 4 余る．
日曜日の数：　7 で割ると 5 余る．
月曜日の数：　7 で割ると 6 余る．

という特徴があることがわかる．

月	火	水	木	金	土	日
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

(2010 年 12 月)

カレンダーに実際に現れる数は 1〜31 だが、この考え方を拡張して数値を順次入れていけば、すべての整数は月〜日のどれかに当てはまる であろう．

すなわち、**任意の整数 n** は

$$\boldsymbol{n = 7k + r,\ \text{ただし}\ r = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6}$$

の**どれかの形**で表される．

このとき、n を 7 で割るときの余り 0, 1, 2, 3, 4, 5, 6 で分けて、表の火〜月に属するすべての整数の集合をそれぞれ $C(0)$, $C(1)$, $C(2)$, $C(3)$, $C(4)$, $C(5)$, $C(6)$ で表して、そのすべてを書き上げてみると

$$C(0) = \{\cdots\cdots, -14,\ -7,\ 0,\ 7,\ 14,\ \cdots\cdots\}$$
$$C(1) = \{\cdots\cdots, -13,\ -6,\ 1,\ 8,\ 15,\ \cdots\cdots\}$$
$$C(2) = \{\cdots\cdots, -12,\ -5,\ 2,\ 9,\ 16,\ \cdots\cdots\}$$
$$C(3) = \{\cdots\cdots, -11,\ -4,\ 3,\ 10,\ 17,\ \cdots\cdots\}$$
$$C(4) = \{\cdots\cdots, -10,\ -3,\ 4,\ 11,\ 18,\ \cdots\cdots\}$$
$$C(5) = \{\cdots\cdots, -9,\ -2,\ 5,\ 12,\ 19,\ \cdots\cdots\}$$
$$C(6) = \{\cdots\cdots, -8,\ -1,\ 6,\ 13,\ 20,\ \cdots\cdots\}$$

となる．そして、この場合は 7 つの集合だが、これらについては

(i) **いずれも空集合でない．**
(ii) **その和集合は整数全体の集合となる．**
(iii) **どの 2 つにも共通の要素がない．**

という性質があり、このような集合を **7 を法とする剰余類**という．

一般に **m を法とする剰余類**は、m で割ったときの余りが 0, 1, 2, $\cdots\cdots$, $m-1$ の m 通りあるので

$$C(0),\ C(1),\ \cdots\cdots, C(m-1)$$

であって、こういう組み分けを**類別**といい、これらの集合をそれぞれ 0, 1, 2$\cdots\cdots$, $m-1$ で代表させ、その「 集合の集合 」を

$$Z_m = \{0,\ 1,\ 2,\ \cdots\cdots,\ m-1\}$$

で表して、**m を法とする剰余系**、あるいは法 m の剰余系、あるいはもっと簡略に m による剰余系などという.

ここで、最も基本的で重要な「 **定理** 」を 1 つあげておく.

連続整数の積

(1) 連続 2 整数の積は 2 の倍数である.

(2) 連続 3 整数の積は 6 の倍数である.

(**解説**) これは、改めて「 定理 」などといわなくても、まあ、ほとんど「 当たり前 」である. そして、これだけを証明するなら、やり方もいろいろある. しかし、ここでシッカリ「 **剰余類**の考え方 」を**標準装備**としてもらいたい.

(1) **連続 2 整数**というと、n と $n+1$ (あるいは $n-1$ と n) という表し方ができるが、基本的にはどちらでも同じだから n と $n+1$ で説明する. その積を N とおくと

$$N = n(n+1)$$

で、この n は**偶数**か**奇数**か、それ以外にはない——そのように**場合分け**をする.

(i) n が偶数のとき、k を適当な整数として $\boldsymbol{n = 2k}$ と表されるから

$$N = 2k(2k+1) \longleftarrow \text{偶数！}$$

(ii) n が奇数のときは、同様に k を適当な整数として $\boldsymbol{n = 2k+1}$ と表されるから

$$N = (2k+1)\{(2k+1)+1\} = 2(2k+1)k \longleftarrow \text{偶数！}$$

いずれの場合も N は偶数、すなわち 2 の倍数である.

(2) **連続 3 整数**というと

$$n,\ n+1,\ n+2 \quad \text{あるいは } n-1,\ n,\ n+1$$

など、連続していればどのようにとってもよいのだが、今度はあとの方でやってみるか.

そうすると

$$N = (n-1)n(n+1)$$

で、これが $6\ (=2\times 3,\ 2$ と 3 は互いに素$)$ の倍数、つまり N が「 **2 の倍数であり、かつ 3 の倍数** 」であることを示さなければならない. しかし、これが 2 の倍数であることはすでに (1) で示されているので、あとは 3 の倍数であることをいえばよい.

ここで整数 n は、k を適当な整数として $3k,\ 3k+1,\ 3k+2$ のいずれか 1 つの形で表されるので、それぞれについて場合を分けて考える.

(i) $\boldsymbol{n = 3k}$ のとき

$$N = (3k-1)(3k)(3k+1) = 3k(3k+1)(3k-1) \longleftarrow \textbf{3 の倍数！}$$

(ii) $\boldsymbol{n = 3k+1}$ のとき

$$N = (3k+1-1)(3k+1)(3k+1+2) = 3k(3k+1)(3k+3) \longleftarrow \textbf{3 の倍数！}$$

(iii) $\boldsymbol{n = 3k+2}$ のとき

$$N = (3k+2-1)(3k+2)(3k+2+1) = 3(3k+1)(3k+2)(k+1) \longleftarrow \textbf{3 の倍数！}$$

となり、いずれも 3 の倍数で、したがって N は 6 の倍数である．

＜ end. ＞

(注 **1**) 剰余類の考え方

(1) は自然数 n を「 **2 を法とする剰余類** 」に、(2) は「 **3 を法とする剰余類** 」に分けることで問題を解決したわけである．

このとき、たとえば (2) の例でいうと

$$n = 3k,\ 3k+1,\ 3k+2$$

ですべての場合を検証した、とした．しかし、この「 $3k+2$ (3 で割って 2 余る数) 」の代わりに「 $3k-1$ (3 で割って 1 足りない数) 」を用いてもよい．それは

$$\begin{aligned} 3k-1 &= 3k-3+3-1 \\ &= 3\underbrace{(k-1)}_{k'}+2 = 3k'+2 \end{aligned}$$

と変形すればよくわかるが、結局、類別された「 同じ剰余類の数 」を検証していることになり、本文に述べたカレンダーの例でいうと、k に連続した 7 個の整数をとれば、「 (月) から (日) までの各々の曜日 」の類の数として、すべての整数を検証したことになる からである．

もう 1 つ注意しておかなくてはならないことがある．それは、たとえば、3 を法とする場合、次の 2 通りの表記の例でいうと

$$\begin{aligned} A &\longrightarrow\ 3k,\ 3k+1,\ \ 3k+2 \\ B &\longrightarrow\ 3k-1,\ \ 3k,\ \ 3k+1 \end{aligned}$$

と表したとしよう．ここで、$k = 1,\ 2,\ 3,\ \cdots\cdots$ とおくと

$$\begin{aligned} &A \text{ の場合} \longrightarrow\ 3,\ 4,\ 5,\ 6,\ 7,\ \cdots\cdots \\ &A \text{ の場合} \longrightarrow\ 2,\ 3,\ 4,\ 5,\ 6,\ \cdots\cdots \end{aligned}$$

となって、A の場合は 1, 2 が入ってこないし、B の場合でも 1 が入ってこないので悩んでしまう人がいる———筆者も昔、そう思ったことがある．

そういうときは便利な言葉があるので教えておこう．それは「 **適当な整数 $\boldsymbol{k}$ をとって** $\cdots\cdots$ 」と書き始めればよい のだ．そうすれば必要に応じて $k = 0$ の場合なども含まれるので、k に対して余計な説明をしなくともハナシは通じることになる．

この場合でいえば「 **適当な整数 $\boldsymbol{k}$ をとれば $\boldsymbol{n = 3k,\ 3k \pm 1}$ とおけて** $\cdots\cdots$ 」などの表現でその意味は十分に尽くされていることになるのである．

ちなみに、7 を法とする場合は「 **適当な整数 $\boldsymbol{k}$ をとれば $\boldsymbol{n = 7k,\ 7k \pm 1,\ 7k \pm 2,\ 7k \pm 3}$ とおけて** $\cdots\cdots$ 」だが、要は、欠落した剰余類がないように、自分の都合に合わせて書けばよい———すべての自然数について検証されたことになる．

(注 **2**) **(2)** について———他の方法もある

この定理を一般化すると

「 **連続 p 個の整数の積は $p!$ の倍数である** 」

となる．これは、n 個の異なるものから r 個とる組合せに数を考えてみると

$$ {}_n\mathrm{C}_r = \frac{\boldsymbol{n(n-1)\cdots\cdots(n-r+1)}}{\boldsymbol{r!}} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*) $$

だが、この右辺の分子 $n(n-1)\cdots\cdots(n-r+1)$ は連続する n 個の積で、左辺はもちろん整数であるから、この分子は $r!$ で割り切れるはずである．

また $(*)$ は、数学的帰納法で証明することもできるが、ここでは触れない———ハナシがわかればそれでよい．そういうわけで、上記の (1) (2) は、$r = 2, 3$ とおけば、その成立は当たり前のことである．

あるいは、数列の公式からアプローチすることもできる．つまり

$$ \sum_{k=1}^{n} k = \frac{n(n+1)}{2} $$

で、左辺はトウゼン整数だから $\dfrac{n(n+1)}{2}$ も整数で、$n(n+1)$ が 2 の倍数であることはほとんど自明であろう．また

$$ \sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3} $$

を思い出せば $n(n+1)(n+2)$ が 3 の倍数であることもさして難しいハナシではない．

そういうことなら、いっそ自然数を

$$ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ \cdots\cdots\cdots\cdots\cdots\cdots $$

と書き並べれば、連続 3 整数をとれば必ずその中に 3 の倍数があるはずだ、と言っても、文句はないだろう．まあ、いろいろな考え方があるが、整数論では本文で述べたように、自然数 n を $3k,\ 3k+1,\ 3k+2$ に分ける「 **剰余類**の考え方 」が重要であることは、改めていうまでもない．

(注) ＜ end. ＞

＜メモ＞

■ 剰余類について

剰余類については、一応の納得が得られたと思うが、「 納得した 」ということと、「 実際に現場でツカエル 」ということはかなりちがうはずである.

そこで、もう少し具体的にハナシをツメておく.

＜ 例 **1** ＞

3 で割って余りが r になるような整数の集合を K_r と書くことにする. $a,\ b,\ c$ をそれぞれ $K_0,\ K_1,\ K_2$ に属する整数とするとき

(1) $a+b,\ 2b+c,\ bc,\ c^3-c$ は、それぞれ $K_0,\ K_1,\ K_2$ のどれに属するか.

(2) $bx+c$ が K_0 に属するような整数 x は、$K_0,\ K_1,\ K_2$ のどれに属するか.

(解)$a,\ b,\ c$ は、それぞれ $K_0,\ K_1,\ K_2$ に属する整数だから $a',\ b',\ c' \in Z$ として

$$a=3a' \quad b=3b'+1, \quad c=3c'+2$$

である――このカタチがポイント！

(1) それぞれ計算すると

$$\begin{aligned}
a+b &= (3a')+(3b'+1) \\
&= 3(a'+b')+1 \in K_1 \ \longleftarrow \ 3 \text{ で割って 1 余る！} \\
2b+c &= 2(3b'+1)+(3c'+2) \\
&= 3(2b'+c'+1)+1 \in K_1 \ \longleftarrow \ 3 \text{ で割って 1 余る！} \\
bc &= (3b'+1)(3c'+2) \\
&= 9b'c'+3(2b'+c')+2 \\
&= 3(3b'c'+2b'+c')+2 \in K_2 \ \longleftarrow \ 3 \text{ で割って 2 余る！} \\
c^3-c &= c(c+1)(c-1) \\
&= (3c'+2)(3c'+2+1)(3c'+2-1) \\
&= 3(3c'+2)(c'+1)(3c'+1) \in K_0 \ \longleftarrow \ 3 \text{ で割りきれる！}
\end{aligned}$$

(2) $x=3x'+r\ (r=0,\ 1,\ 2)$ とおくと

$$\begin{aligned}
bx+c &= (3b'+1)(3x'+r)+(3c'+2) \\
&= 3(3b'x'+b'r+x'+c')+\boldsymbol{(r+2)}
\end{aligned}$$

ここで $bx+c \in K_0$ であるためには $\boldsymbol{r+2 \in K_0}$ でなければならないが、r のとり得る値は $r=0,\ 1,\ 2$ だから、適するものは $r=1$ で、したがって $x \in K_1$ である.

＜ end. ＞

＜例 **2**＞

自然数 $a,\ b,\ c,$ の間に

$$a^2+b^2=c^2 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

が成り立つものとする．

(1) $a=7$ のとき、 $b,\ c$ の値を求めよ．

(2) 3 数 $a,\ b,\ c,$ が 1 以外の正の公約数をもたないとき、$a,\ b$ のうち 1 つは偶数で、他の 1 つは奇数であることを証明せよ．

(解) (1) $a=7$ であるから $(*)$ は $b,\ c$ についての**不定方程式**である．

a を代入すると

$$7^2+b^2=c^2 \qquad \therefore\ \ c^2-b^2=49 \qquad \therefore\ \ (c+b)(c-b)=49$$

ここで、 $c+b$ は正整数だから $c-b$ も正整数で、$0<c-b<c+b$ もいえるから

$$\begin{cases} c+b=49 \\ c-b=1 \end{cases} \qquad \therefore\ \ b=24,\ \ c=25$$

(2) m を整数とすると

$$(2m)^2=4m^2, \qquad (2m-1)^2=4(m^2-m)+1$$

だから、ここでは **(偶数)^2** と **(奇数)^2** が $(*)$ の左辺でどのように絡んでくるかを見極める．

証明を求められているのは 「 **$a,\ b$ のうち 1 つは偶数で、他の 1 つは奇数である** 」ということだから、**背理法**を使って「 $a,\ b$ ともに偶数 」の場合と「 $a,\ b$ ともに奇数 」の場合が否定されればよい．すなわち

(i) a, b がともに偶数とすると、$(*)$ の左辺の a^2+b^2 は 4 の倍数だから、c は偶数である．

$\longrightarrow$ $a,\ b,\ c$ は 1 以外の正の公約数 2 をもつから不適！

(ii) a, b がともに奇数とすると、$(*)$ の左辺の a^2+b^2 は 4 で割ると 2 余る数である．

$\longrightarrow$ $(*)$ の右辺の c^2 は、c が偶数でも奇数でもこうはならない．

で、いずれも $(*)$ は成立しない．

したがって、$a,\ b$ の少なくとも一方は偶数で、他方は奇数である．

★$_1$ ピタゴラス数

$\boldsymbol{a^2+b^2=c^2}$ を満たす正整数 $a,\ b,\ c$ を**ピタゴラス数**という――なかなかおもしろい性質があるので注目しておきたい．特に本文でも強調したが

「 **$a,\ b$ のうち 1 つは偶数で、他の 1 つは奇数である** 」

このことから **c が奇数**であることもわかる．これらは**特記事項**である――あとで使うことになる．また、上記で

「 $a,\ b$ のうち 1 つは偶数で、他の 1 つは奇数 $\cdots\cdots$ 」

としたところを

「 **$a,\ b$ のうち 1 つは 3 の倍数で、他の 1 つは 3 の倍数でない $\cdots\cdots$** 」

と書き換えても成り立つことも知っておくとよい．それは

$$(3m\pm1)^2=3(3m^2\pm6m)+1$$

だから、「 3 の倍数でない数を 2 乗して 3 で割ると 1 余る 」ことを表している――「 2 の倍数のとき 」と全く同様に証明することができる．あるいは

「 **$a,\ b$ のうち 1 つは 4 の倍数である $\cdots\cdots$** 」

ことも証明することができる．

これは、先に述べた $a,\ b$ のどちらかが奇数、他方が偶数といったとき、たとえば a を奇数、b を偶数とすると、「 b が 4 の倍数でない偶数 $2(2m-1)$ のカタチではダメである 」ことをいえばよい．それには

$$\begin{aligned}(2m-1)^2 &= 4(m^2-m)+1\\ &= 4\underbrace{m(m-1)}_{2\text{ の倍数}}+1 = 8M_1+1 \ \longleftarrow\ \text{連続 2 整数の積は 2 の倍数！}\end{aligned}$$

だが、4 の倍数でない偶数は $2(2m-1)$ だからこの 2 乗は

$$\begin{aligned}\{2(2m-1)\}^2 &= 4(2m-1)^2\\ &= 4(4m^2-4m+1) = 16M_2+4\end{aligned}$$

そこで、a が奇数、b が 4 の倍数でない偶数のとき、$(*)$ の左辺は

$$\begin{aligned}a^2+b^2 &= (8M_1+1)+(16M_2+4)\\ &= 8(M_1+2M_2)+5 \ \longleftarrow\ \textbf{8 で割ると 5 余る！}\end{aligned}$$

このとき、右辺の c は奇数だから $c^2 = 8M_3+1$ で結局 $(*)$ は成り立たない．だから、「 $a,\ b$ のうち 1 つは 4 の倍数である 」ことがいえた．まあ、ハナシとしてはこの辺でよかろう．

字面で見ると結構タイヘンに見えるかも知れないが、後で述べる**合同式**を用いて書くといくらかスッキリ書けるかと思う——それは読者にお任せする．

★$_2$ ピタゴラス数の拡張

さらに、本問は次のように拡張できる．すなわち

「 正整数 $a,\ b,\ c,\ d$ の間に

$$a^2+b^2+c^2=d^2$$

が成り立つとき、$a,\ b,\ c,\ d$ のうち少なくとも 2 つは偶数である.」

だが、これについてはここでは触れない——そんなものか、と思ってもらえば十分である．

＜ end. ＞

1.2.3.2　合同式

ここで、いきなり「 **合同式** 」といわれても、初学者としては何のことやら、何が有難いのかわからない、というのが実情であろう．まずは「 合同式とは何か 」、「 何が有難いのか 」を説明し、「実際に使ってみせる」という手順で解説する．

＜1＞ 合同式とは何か

前掲のカレンダーでわかるように、すべての整数は「 火曜日から月曜日 (1 週間分) の 7 個の類 」のどれかに**類別される**、すなわち、7 で割るとその余りは 0, 1, 2, 3, 4, 5, 6 のどれかになるであろうことは容易に納得してもらえたと思う．

これを一般化すると、「 **m を法とする剰余類** 」を

$$K_0,\ K_1,\ \cdots\cdots,\ K_{m-1}$$

とし、たとえば 2 つの類 $K_i,\ K_j$ からそれぞれ $a,\ b$ をとると

$$a \in K_i \quad \Longrightarrow \quad a = mq_1 + i$$
$$b \in K_j \quad \Longrightarrow \quad b = mq_2 + j$$

ここで、$a \pm b,\ ab$ を計算してみると

$$\boldsymbol{a \pm b} = \underbrace{m(q_1 \pm q_2)}_{m\ \text{で割れる！}} + (\boldsymbol{i \pm j}) \ \longleftarrow \ \text{複号同順！}$$
$$\begin{aligned}\boldsymbol{ab} &= (mq_1 + i)(mq_2 + j) \\ &= \underbrace{m^2 q_1 q_2 + m(q_1 j + q_2 i)}_{m\ \text{で割れる！}} + \boldsymbol{ij}\end{aligned}$$

であるから、「 $\boldsymbol{a \pm b,\ ab}$ がどの類に属するか 」を見るには、上記の m の倍数の部分は関係なくて、「 $\boldsymbol{i \pm j,\ ij}$ のところだけを調べればよい 」ことがわかる．

いま、x と y が m を法とする同じ剰余類に属する、すなわち $x - y$ が m の倍数になることを

$$\boldsymbol{x \equiv y \pmod{m}} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

と書くことにすれば、上記の事情は

$$\boldsymbol{a \pm b \equiv i \pm j \pmod{m}} \ \longleftarrow \ \text{複号同順！}, \quad \boldsymbol{ab \equiv ij \pmod{m}}$$

という表し方ができる．つまり、もはや $mq_1,\ mq_2$ などを計算に引きずる必要はなく、$i,\ j$ の計算のみで済ますことができる――ここが**有難い**のだ

そして、この 3 本線の記号「 $\equiv$ 」を「 **合同** 」の記号といい、① のような擬似的な等式を**合同式**という．要するに、**合同式**は、整数論の基本概念である**整除性**を記号的に表したもので、合同の概念を始めてとりいれたのは**ガウス (C.F.Gaus 1777〜1855　ドイツ)** であるといわれている．

われわれの立場は、この**整除性**について、**0** や**負の数**もとりいれてきたが、**合同式**を扱うようになると、正の整数の理論を作るより、その方がずっと**便利**で**発展的**に扱えることを実感してもらえると思う．

＜2＞ 合同式の代数

合同式は、確かに便利ではあるが、気分的にちょっと「 敷居が高い 」ので使い慣れるまで注意が必要である．答案などでも、合同式を使って書いてあると、「 いかにもスマートでカッコいい 」のだが、それで間違えたのでは目も当てられない——以下、筆者も気合を入れて書くから、そのつもりで読んでもらいたい．

さて、合同式だが、それは、われわれが代数で用いる等式 $x = y$ とよく似た性質を持っている．いわば、**整数論の代数**であると考えればよい．

たとえば

$$
\begin{array}{ll}
1^\circ & a \equiv a \pmod{m} \\
2^\circ & a \equiv b \implies b \equiv a \pmod{m} \\
3^\circ & a \equiv b,\ \ b \equiv c \implies a \equiv c \pmod{m}
\end{array}
$$

が成り立つ．

これは等式の場合と全く同じである——「 等しい 」ということは、この「 合同 」の「 特別な場合である 」と考えてもよい．

つまり、$a = b$ というのは、任意の整数 m を法として $a \equiv b \pmod{m}$ に他ならない．そういう理解の上で、さらに「 **合同の 加法、減法、乗法** 」はどうなるのか．

まず、次の定理が成り立つ．

定理 1

$a \equiv b,\ c \equiv d \pmod{m}$ のときは、次の合同式が成り立つ．

(1) $a \pm c \equiv b \pm d \pmod{m}$　　(2) $ac \equiv bd \pmod{m}$

ただし、複号は同順である．

(**証明**) (1) 条件から

$$
\begin{array}{l}
a \equiv b \pmod{m} \longrightarrow a - b = mk \\
c \equiv d \pmod{m} \longrightarrow c - d = ml
\end{array}
$$

であるから、以下複号同順で

$$
\begin{aligned}
(a \pm c) - (b \pm d) &= (a - b) \pm (c - d) \\
&= m(k \pm l) \longleftarrow (k \pm l) \text{ は整数！} \\
\therefore\ \ a \pm c &\equiv b \pm d \pmod{m}
\end{aligned}
$$

(2) 差をとれば

$$
\begin{aligned}
ac - bd &= (a - b)c + (c - d)b \\
&= m(kc + lb) \longleftarrow (kc + ld) \text{ は整数！} \\
\therefore\ \ ac &\equiv bd \pmod{m}
\end{aligned}
$$

＜end.＞

(注) 「 系 」——定理を補足する「 準定理 」

この定理の特別な場合として $c = d = p$ の場合を考えると

系 1	$a \pm p \equiv b \pm p \pmod{m}$
系 2	$ap \equiv bp \pmod{m}$

が成り立つ．

これは等式の場合と同様に、合同式でも その両辺に同じ整数を加えてもひいてもよく、さらに同じ整数をかけてもよい、ということを表している．

したがって、等式の場合と同様に、両辺に $(-b)$ を加えて

$$a+b\equiv c \implies a\equiv c-b \pmod{m}$$

などの変形ができる．すなわち、符号を変えて「 **移項する** 」という操作ができる のである．

また、上記の「 定理 **1** (2) 」の特別な場合として、 $a=c,\ b=d,\ n$ を正整数 とすると

系 3　$a\equiv b \implies a^n\equiv b^n \pmod{m}$

が成り立つ．なぜなら、上記の「 **定理 1** (2) 」の $ac\equiv bd$ で、$c=a,\ d=b$ とすれば

$$a\equiv b \implies a^2\equiv b^2 \pmod{m}$$

となり、これを繰り返して用いると、合同式の 両辺は何乗してもよい ことがわかる．

ただし、普通の等式の場合とちがって、無条件に両辺を同じ整数 $(\neq 0)$ で割ることはできない．たとえば、 $12\equiv 4 \pmod{8}$ だが、両辺を 2 で割って $6\equiv 2 \pmod{8}$ 、あるいは 4 で割って $3\equiv 1 \pmod{8}$ とはできない．

しかしこの場合でも、mod 8 の数値 8 も同時に 2, 4 で割って、$6\equiv 2 \pmod{4}$ 、あるいは $3\equiv 1 \pmod{2}$ ならば成り立つ．これについては次の「 定理 2 」をみてもらいたい．

＜ end. ＞

定理 2

$ac\equiv bc \pmod{m}$ で、**m と c が互いに素**であれば、 $a\equiv b \pmod{m}$ である．

(**証明**) 条件から

$$ac-bc=(a-b)c=mk \ (k \text{ は整数})$$

であるから、c と m が互いに素なら $a-b$ が m の倍数、すなわち $a\equiv b \pmod{m}$ が得られる．前掲の (**注**) で述べた例は、m と c が互いに素でない場合のハナシであって、もし $4\equiv 48 \pmod{11}$ の 4 と 11 のように、互いに素であるときは、両辺を 4 で割って $1\equiv 12 \pmod{11}$ とすることができる——この定理はこういうことを主張しているのである．

＜ end. ＞

定理 3

$a\equiv b \pmod{m}$ の右辺 (または左辺) に km(k は任意の整数) を加えて

$$a\equiv b+km \pmod{m}$$

が成り立つ．

(**証明**) この定理は、普通の等式の場合とは少しちがうが、合同の定義から考えて「 その成立は明らか 」としてよかろう．

たとえば

$$17\equiv 361 \pmod{8} \implies 17\equiv 361-8\times 45=1 \pmod{8}$$

のような計算ができるのである——合同式の便利な点の 1 つであろう．

＜ end. ＞

＜メモ＞

■ 合同式入門――まずわかり、そして慣れよ

何でもそうだが、理屈ではわかっていても使いこなすのはなかなかホネである．まず、その有難さを実感しないことには本気にはなれまい．

次の例題はそれを実感してもらうためのものだと思ってもらいたい．では早速はじめよう．

＜例＞

(1) 整数 a が 3 で割り切れないとき、ax が、任意の整数 b と、3 を法とする同じ剰余類に属するような整数 x が存在することを証明せよ．

(2) 6 で割ると 5 余る正の整数を p とするとき、p^{2n+1} もまた、6 で割ると 5 余ることを証明せよ．ただし、n は正の整数とする．

(解) (1) まず、これはどういう意味か．

「 ax と b とが、3 を法とする同じ剰余類に属する 」ということは、「 ax と b は 3 で割るときの余りが等しい 」ということである．言い換えれば「 $ax-b$ が 3 の倍数である 」ということ、したがって、これを合同式で表すと「 $\boldsymbol{ax \equiv b \pmod 3}$ 」ということである．

ここで、合同式の知識がなければ、仕方がないからシコシコやる しか方法はない――まずはそれでやってみる．

条件は、「 $ax-b$ が 3 の倍数 」だから

$$ax-b=3k \ (k \text{ は整数})$$

となる x があることをいえばよい．

そこで a だが、これは 3 の倍数ではないから、m を適当な整数として

$$a=3m+1, \text{ または } 3m+2$$

と表される．

(i) $\boldsymbol{a=3m+1}$ **のとき：**

$$\begin{aligned} ax-b &= (3m+1)x-b \\ &= 3mx+(x-b) \cdots\cdots ① \end{aligned}$$

で、この右辺が 3 の倍数になるような x があるか、ということをきいている．そこで

$$x-b=3m' \quad \therefore \quad x=3m'+b$$

これを ① に入れると

$$ax-b=3mx+3m'=3(mx+m') \longleftarrow \text{ 3 の倍数になった！}$$

すなわち、$x=3m'+b$ として存在する．

(ii) $\boldsymbol{a=3m+2}$ **のとき：**

$$\begin{aligned} ax-b &= (3m+2)x-b \\ &= 3mx+(2x-b) \\ &= 3(m+1)x-(x+b) \cdots\cdots ② \end{aligned}$$

で、この右辺が 3 の倍数になるような x があるか、ということをきいているのである．

そこで、この右辺が 3 の倍数となるように x を決めればよいから

$$x+b=3m' \quad \therefore \quad x=3m'-b$$

これを ② に入れると

$$ax-b=3(m+1)x-3m'=3\{(m+1)x-m'\} \longleftarrow \text{ 3 の倍数になった！}$$

すなわち、$x=3m'-b$ として存在する．

結局、(i) (ii) のいずれの場合も条件を満たす x が存在する．と、まあこんなものだが、**結構タイヘン**である．しかし、**合同式の知識**があれば

$$\boldsymbol{ax \equiv b \pmod 3}$$

を満たす x があるか、ときいているのだから

まず (i) の $\boldsymbol{a = 3k + 1}$ **のとき**ならば

$$ax = (3k+1)x \equiv b \pmod 3$$

前掲の「 **定理 3** 」にしたがって、左辺に 3 の倍数である $(-3kx)$ を加えると

$$(3k+1)x + (-3kx) \equiv b \pmod 3 \qquad \therefore \quad x \equiv b \pmod 3$$

そこで、$x - b = 3l$ (l は整数) とおくと、「 $x = b + 3l$ (あった !) 」として $ax \equiv b \pmod 3$ を満たす x があることがわかる——これで「 **一丁あがり！** 」なのだ．

(ii) の $\boldsymbol{a = 3k + 2}$ **のとき**も同様にやればよい．

(2) こういう問題こそ、「 **合同式の有難さ** 」が身にしみる．それを実感してもらうために、まずは、まだ合同式の知識がないものとしてやってみよう．

p は 6 で割ると 5 余るので

$$p = 6m + 5 = 6\underbrace{(m+1)}_{k\ \text{とおく}} - 1 \quad \longleftarrow \quad \text{扱う数値を小さくしておく!}$$

$$= 6k - 1 \quad (k\ \text{は整数})$$

と表せる．そこで

$$\begin{aligned} p^{2n+1} &= (6k-1)^{2n+1} \quad \longleftarrow \quad \text{2 項定理で展開する！} \\ &= \underbrace{(6k)^{2n+1} - {}_{2n+1}\mathrm{C}_1(6k)^{2n} + \cdots\cdots + {}_{2n+1}\mathrm{C}_{2n}(6k)}_{6N\ \text{とおく}} - 1 \\ &= 6N - 1 \quad \longleftarrow \quad \text{6 で割ると 5 余るカタチに変形する！} \\ &= 6(N-1) + 5 \quad \longleftarrow \quad \text{変形デキタ！} \end{aligned}$$

で、まあ一件落着だが、いつもこれではとてもタイヘンだろう．これを「 **合同式でやる** 」とどうなるか——実は、こういうのは合同式の得意科目なのです．

p は 6 で割って 5 余るので

$$p \equiv 5 \pmod 6$$

この右辺に (-6) を加えると

$$p \equiv 5 - 6 = -1 \pmod 6$$

「 **定理 1 の系 3** 」を用いて、両辺を $(2n+1)$ 乗 すると

$$p^{2n+1} \equiv (-1)^{2n+1} = -1 \pmod 6$$

「 **定理 3** 」により、右辺に 6 を加えて

$$p^{2n+1} \equiv -1 + 6 = 5 \pmod 6$$

すなわち、p^{2n+1} も 6 で割ると 5 余ることが証明された——これで**オシマイ！**

「 合同式でやる 」のははいかがですか．

＜ end. ＞

＜3＞ 合同式の演習

合同式の理論そのものは、そう難しいものではないし、また前掲の定理や系を知っているだけでもかなり広い範囲にわたって応用できる.

まあ、便利に使えるものは積極的に使おうではないか——ここでは、少し練習をしてみることにする.

＜メモ＞

■ 合同式の演習

＜ 例 1 ＞

ある整数 N について、次のことがらを証明せよ.

(1) 2 の倍数である条件は、1 位の数が偶数であることである.

(2) 4 の倍数である条件は、下 2 桁の数が 4 の倍数であることである.

(3) 8 の倍数であるための条件は、下 3 桁が 8 の倍数であることである.

(4) 3, 9 の倍数であるための条件は、各位の数の和が、それぞれ 3, 9 の倍数であることである.

(5) 11 の倍数であるための条件は、「奇数番目の数の和」と「偶数番目の数の和」との差が 11 の倍数であることである.

(解) よく融合問題で使われたりするテーマだが、どれもポピュラーで、すべて**定理**と思ってよい.

一般に、10 進法の n 桁の整数は

$$\boldsymbol{N = a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots\cdots + a_{n-1} \cdot 10 + a_n} \cdots\cdots\cdots ①$$

(ただし、 $1 \leqq a_1 \leqq 9, \quad 0 \leqq a_2, \cdots\cdots a_{n-1}, a_n \leqq 9$)

であることはすでに述べた――まず、これをシッカリとアタマにたたき込んでおくべし.

(1) これは、もう証明もヘッタクレもない当たり前のことだが、まず、これを合同式で表す.

$$N = \underbrace{a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots\cdots + a_{n-1} \cdot 10}_{10M_1 \text{とおく}} + a_n$$

$$= 10M_1 + a \longleftarrow a_n \text{を } a \text{ とおいた！}$$

そうすると $\boldsymbol{10 \equiv 0 \pmod 2}$ だから

$$\boldsymbol{N = 10M_1 + a \equiv a \pmod 2} \longleftarrow 10M_1 \text{はすでに 2 の倍数！}$$

ゆえに、a が 2 の倍数なら N も 2 の倍数である.

(2) 下 2 桁とあるから、3 桁以上に注目すると $10^2 = 100$ は $2^2 = 4$ の倍数 で、したがって、これ以上の部分はすでに 4 の倍数になっているから、相手にしなくてよい.

$$N = \underbrace{a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots\cdots + a_{n-2} \cdot 10^2}_{10^2 M_2 \text{とおく}} + a_{n-1} \cdot 10 + a_n$$

$$= 10^2 M_2 + 10b + a \longleftarrow a_n,\ a_{n-1} \text{を } a,\ b \text{ とおいた！}$$

そうすると $\boldsymbol{10^2 \equiv 0 \pmod 4}$ だから

$$\boldsymbol{N = 10^2 M_2 + 10b + a \equiv 10b + a \pmod 4} \longleftarrow 10^2 M_2 \text{はすでに 4 の倍数！}$$

ゆえに、$10b + a$ が 4 の倍数なら N も 4 の倍数である.

(3) 上記のハナシは下 3 桁でも同様である. つまり $10^3 = 1000$ は $2^3 = 8$ の倍数 だから

$$N = \underbrace{a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots\cdots + a_{n-3} \cdot 10^3}_{10^3 M_3 \text{とおく}} + a_{n-2} \cdot 10^2 + a_{n-1} \cdot 10 + a_n$$

$$= 10^3 M_3 + c10^2 + 10b + a \longleftarrow a_n,\ a_{n-1},\ a_{n-2} \text{を } a,\ b,\ c \text{ とおいた！}$$

そうすると $\boldsymbol{10^3 \equiv 0 \pmod 8}$ だから

$$\boldsymbol{N = 10^3 M_3 + 10^2 c + 10b + a \equiv 10^2 c + 10b + a \pmod 8}$$

$$\longleftarrow 10^3 M_3 \text{はすでに 8 の倍数！}$$

ゆえに、$10^2 c + 10b + a$ が 8 の倍数なら N は 8 の倍数である.

(4) n 桁の整数 N は

$$\begin{aligned} N =& a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots + a_k \cdot 10^{n-k} \cdots + a_{n-1} \cdot 10 + a_n \\ =& \sum_{k=1}^{n} a_k \cdot 10^{n-k} \end{aligned}$$

ここで、「 $\boldsymbol{10^k \equiv 1 \pmod 3}$ **($\boldsymbol{k}$ は任意の整数)** 」から、k を n より大きくない整数として

$$10^{n-k} \equiv 1 \pmod 3 \qquad \therefore \quad a_k \cdot 10^{n-k} \equiv a_k \pmod 3$$

$$\therefore \quad N = \sum_{k=1}^{n} a_k \cdot 10^{n-k} \equiv \sum_{k=1}^{n} a_k \pmod 3 \quad (= \boldsymbol{S} \text{ とおく}) \longleftarrow \text{各位の数の和！}$$

したがって、「 各位の数の和 $\boldsymbol{S}$ 」が 3 の倍数なら N も 3 の倍数である.

また、k を n より大きくない整数として

$$10^{n-k} \equiv 1 \pmod 9$$

だから、上と同様にして「 各位の数の和 $\boldsymbol{S}$ 」が 9 の倍数なら N も 9 の倍数である ことがいえる———なかなか巧いものである.

(5) こうなるとなかなか難しい———この場合、10 の奇数乗と偶数乗でハナシがちがうのだ.

そこで、まず最初に

$$\boldsymbol{10^{2k-1} \equiv -1 \pmod{11}}, \quad \boldsymbol{10^{2k} \equiv 1 \pmod{11}}$$

に気がつくか———わかりにくければ、$10^3 = 1000$, $10^2 = 100$ などを実際に 11 で割って余りを確かめてみるとよい.

そこで、改めて ① をながめてみよう.

$$N = a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + \cdots\cdots + a_{n-1} \cdot 10 + a_n$$

まず、n が偶数のときは

$$\begin{aligned} N \equiv& -a_1 + a_2 - \cdots\cdots - a_{n-1} + a_n \\ =& -\underbrace{(a_1 + a_3 + \cdots + a_{n-1})}_{\frac{n}{2}\text{個}} + \underbrace{(a_2 + a_4 + \cdots + a_n)}_{\frac{n}{2}\text{個}} \pmod{11} \end{aligned}$$

n が奇数のときは

$$\begin{aligned} N \equiv& a_1 - a_2 + \cdots\cdots - a_{n-1} + a_n \\ =& \underbrace{(a_1 + a_3 + \cdots + a_n)}_{\frac{n+1}{2}\text{個}} - \underbrace{(a_2 + a_4 + \cdots + a_{n-1})}_{\frac{n-1}{2}\text{個}} \pmod{11} \end{aligned}$$

すなわち、「 奇数番目の数の和 」と「 偶数番目の数の和 」との差が 11 の倍数ならば N も 11 の倍数である.

＜ end. ＞

＜例 **2**＞

n を 4 の倍数でない正整数とするとき

$$p = 1^n + 2^n + 3^n + 4^n$$

は 5 の倍数である．このことを証明せよ．

(解) どこから手をつけるか——「 **5 の倍数** 」とあるぞ．

$$\mathbf{5 \equiv 0 \pmod 5} \longrightarrow \mathbf{4 \equiv -1 \pmod 5}, \quad \mathbf{3 \equiv -2 \pmod 5}$$

だから、4^n, 3^n を計算するとしても、n の偶数、奇数で様子がちがってくる．

そうすると場合を分けて計算することになる．

(i) n が奇数のとき：

$$\mathbf{4 \equiv -1 \pmod 5} \quad \therefore \ \mathbf{4^n \equiv (-1)^n = -1 \pmod 5} \cdots\cdots ①$$

同様にして

$$\mathbf{3 \equiv -2 \pmod 5} \quad \therefore \ \mathbf{3^n \equiv (-2)^n = -2^n \pmod 5} \cdots\cdots ②$$

② + ① より

$$3^n + 4^n \equiv (-2^n) + (-1) \pmod 5 \quad \therefore \ \underbrace{1^n + 2^n + 3^n + 4^n}_{p} \equiv 0 \pmod 5$$

ゆえに、p は 5 で割り切れる．

(ii) n が偶数のとき： n は 4 の倍数でないから、$n = 2m$ (m は奇数) とおくと

$$\begin{aligned} p &= 1^n + 2^n + 3^n + 4^n \\ &= 1^{2m} + 2^{2m} + 3^{2m} + 4^{2m} = 1^m + 4^m + 9^m + 16^m \end{aligned}$$

ここで

$$\mathbf{4 \equiv -1 \pmod 5} \quad \therefore \ \mathbf{4^m \equiv (-1)^m = -1 \pmod 5}$$

$$\therefore \ 1^m + 4^m \equiv 0 \pmod 5 \cdots\cdots ③$$

ここで、 $\mathbf{25 = 9 + 16 \equiv 0 \pmod 5}$ であることに気がつくと

$$\mathbf{9 \equiv -16 \pmod 5} \quad \therefore \ \mathbf{9^m \equiv (-16)^m = -16^m \pmod 5}$$

$$\therefore \ 9^m + 16^m \equiv 0 \pmod 5 \cdots\cdots ④$$

③ + ④ より

$$\underbrace{1^m + 4^m + 9^m + 16^m}_{p} \equiv 0 \pmod 5$$

ゆえに、p は 5 で割り切れる．

＜ end. ＞

＜例 **3**＞

$m,\ n$ を正整数とするとき、n^{m+4}と n^m の 1 の位の数は等しい．これを証明せよ．

(解)「 1 の位の数が等しい 」ということは、「 差をとると 10 の倍数になる 」ということである．そして、この逆も成り立つ．そこで

$$n^{m+4} - n^m = n^m(n^4 - 1) \quad (= p \text{ とおく})$$

これが 10 の倍数、すなわち「 **2 の倍数であり、かつ 5 の倍数** 」であることがいえればよい．

(i) 2 の倍数であることの証明

n は偶数 $(2k)$ か奇数 $(2k+1)$ だから、これを**合同式**で表すと

$$\underbrace{n \equiv 0 \pmod 2}_{A}, \quad \text{または} \quad \underbrace{n \equiv 1 \pmod 2}_{B}$$

である．そこで

$$A \text{ のとき：} \quad n^m \equiv 0 \pmod 2 \qquad \therefore \quad p \equiv 0 \pmod 2$$

$$B \text{ のとき：} \quad n^4 \equiv 1 \pmod 2 \qquad \therefore \quad (n^4 - 1) \equiv 0 \pmod 2 \qquad \therefore \quad p \equiv 0 \pmod 2$$

ゆえに、p は 2 の倍数である．

(ii) 5 の倍数であることの証明

$n = 5k,\ 5k \pm 1, 5k \pm 2$ であるから、それぞれについて確かめればよい．これらのことがらを**合同式**で表すと

$$\underbrace{n \equiv 0 \pmod 5}_{C}, \quad \text{または} \quad \underbrace{n \equiv \pm 1 \pmod 5}_{D}, \quad \text{または} \quad \underbrace{n \equiv \pm 2 \pmod 5}_{E}$$

であるから、それぞれについて確かめればよい．つまり

$$C \text{ のとき：} \quad n^m \equiv 0 \pmod 5 \qquad \therefore \quad p \equiv 0 \pmod 5$$

$$D \text{ のとき：} \quad n^4 \equiv 1 \pmod 5 \qquad \therefore \quad n^4 - 1 \equiv 0 \pmod 5 \qquad \therefore \quad p \equiv 0 \pmod 5$$

$$E \text{ のとき：} \quad n^4 \equiv (\pm 2)^4 = 16 \pmod 5 \qquad \therefore \quad n^4 - 1 \equiv 15 \pmod 5$$

$$\therefore \quad n^4 - 1 \equiv 0 \pmod 5 \qquad \therefore \quad p \equiv 0 \pmod 5$$

ゆえに、p は 5 の倍数である．

以上の考察から p は $2 \times 5 = 10$ の倍数で、条件は証明された．

＜ end. ＞

■ ハイレベルなテーマへの挑戦

せっかくここまで来たのだから、ちょっとハイレベルなテーマに触れておこう．合同式ナシではすまされないことをわかってもらえれば、まあ目的は達成である．

＜例 1＞

p が素数で、a と p が互いに素のときは、a^{p-1}を p で割ると 1 余ることを示せ．
ただし、a は正整数である．

(フェルマーの小定理)

(解) いろいろな証明方法があるが、ここでは **2 項定理** を用いる方法をあげておこう．

そのためには、1 つ定理を準備しておかなければならない．それは

> $m,\ n$ が任意の正整数で、p が素数のときは
> $$\boldsymbol{(m+n)^p \equiv m^p + n^p \pmod{p}}$$
> である．

2 項定理によれば

$$\begin{aligned}(m+n)^p &= {}_p\mathrm{C}_0 m^p n^0 + {}_p\mathrm{C}_1 m^{p-1} n^1 + {}_p\mathrm{C}_2 m^{p-2} n^2 + \cdots\cdots + {}_p\mathrm{C}_1 m^1 n^{p-1} + {}_p\mathrm{C}_p m^0 n^p \\ &= m^p + n^p + \underbrace{\{{}_p\mathrm{C}_1 m^{p-1} n^1 + {}_p\mathrm{C}_2 m^{p-2} n^2 + \cdots\cdots + {}_p\mathrm{C}_1 m^1 n^{p-1}\}}_{A}\end{aligned}$$

で、この A の部分を何とかしなくてはならないが

$$\begin{aligned}{}_p\mathrm{C}_r &= \frac{p(p-1)\cdots(p-r+1)}{r!} \qquad (1 \leqq r \leqq p-1) \\ &= p \cdot \frac{(p-1)\cdots(p-r+1)}{r!} \quad \longleftarrow \ p \text{ を 1 つ前に出す！}\end{aligned}$$

ここで、p は素数であるから、2, 3, $\cdots\cdots$, r のいずれとも互いに素である．

一方、${}_p\mathrm{C}_r$ は整数であるから、分子の $(p-1)\cdots(p-r+1)$ は分母の $r!$ で割り切れなくてはならない．そこで

$$\boldsymbol{\frac{(p-1)\cdots(p-r+1)}{r!} = k \ (\text{整数})}$$

とおくことができて ${}_p\mathrm{C}_r = pk$ となる．すなわち

$$\boldsymbol{{}_p\mathrm{C}_r \equiv 0 \pmod{p} \quad (r = 1,\ 2,\ \cdots,\ p-1)}$$

ゆえに

$$(m+n)^p - (m^p + n^p) = A \equiv 0 \pmod{p} \qquad \therefore \ (m+n)^p \equiv m^p + n^p \pmod{p}$$

が得られる．このことから

$$\begin{aligned}&m = n = 1 \ \longrightarrow \ 2^p \equiv 2 \pmod{p} \\ &m = 2,\ n = 1 \ \longrightarrow \ 3^p \equiv 2^p + 1 \pmod{p} \qquad \therefore \ 3^p \equiv 2 + 1 = 3 \pmod{p}\end{aligned}$$

以下、$m = 3,\ n = 1$ とおけば、同様にして $4^p \equiv 4 \pmod{p}$ が得られ、これを繰り返して

$$\boldsymbol{a^p \equiv a \pmod{p}} \quad \text{ただし、} a \text{ は任意の整数！}$$

が得られる――数学的帰納法で証明すればよい．以上、まとめると

> 任意の正整数 a と、任意の素数 p に対して
> $$\boldsymbol{a^p \equiv a \pmod{p}}$$

だが、a と p が互いに素であるときは、「定理 2」により、両辺を a で割って $\boldsymbol{a^{p-1} \equiv 1 \pmod{p}}$ が得られるのである．

＜ end. ＞

＜例 **2**＞

ピタゴラスの 3 角形の 3 辺の積は 60 で割り切れる．このことを証明せよ．

(解) ピタゴラス 3 角形の 3 辺というのは

$$\boldsymbol{x^2+y^2=z^2} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

を満足する 3 つの整数の組 $(x,\ y,\ z)$ をピタゴラスの 3 数という——これはすでに述べた．

さて、① の解は無数にある．たとえば、「 $x,\ y,\ z$ の最大公約数が 1 」である場合の典型的な解の 1 組として、$x=3,\ y=4,\ z=5$ があるが、これは、k を任意の整数として

$$x=3k,\ y=4k,\ z=5k$$

はすべて ① を満たす組をすべて包括することになる．

しかし、この (3, 4, 5) のような「 $x,\ y,\ z$ の最大公約数が 1 」である組が他にないかというと、実はたくさんあって、斜辺 z が 100 を超えないものだけでも

$$(5,\ 12,\ 13),\quad (7,\ 24, 25),\quad (8,\ 15,\ 17),\quad (9,\ 40,\ 41),\quad (11,\ 60,\ 61)$$
$$(12,\ 35,\ 37),\quad (13,\ 84,\ 85),\quad (20,\ 21,\ 29),\quad (28,\ 45,\ 53),\quad (33,\ 56,\ 65)$$

の 10 通りがあり、① の**一般解**としては、これらの 1 つ 1 つについて、たとえば $(5k,\ 12k,\ 13k)$ のように無数にあることになる．

そして、この問題は、これらの 3 辺の積のすべてが 60 で割り切れるということの証明を要求しているのである——しかし、どこから手をつければよいか．

そこで、① をどうみるか——これを**ピタゴラス方程式**というのだが、どうやら ハナシはこの不定方程式 ① を解くことに収斂するようである．

さて、ここで条件をもう少し絞り込んでおきたい．はじめに「 $x,\ y,\ z$ の最大公約数が 1 」と書いたが、実は「 $\boldsymbol{x,\ y,\ z}$ **のどの 2 つも互いに素** 」になっているのである．

たとえば、「 素数 p が $x,\ y$ の公約数で、p が z の約数でない場合があるか 」ということだが、$x=pa,\ y=pb$ とおいて ① に代入してみると

$$(pa)^2+(pb)^2=z^2 \qquad \therefore\ \ p^2(a^2+b^2)=z^2 \ \longleftarrow\ \boldsymbol{z}\ \text{が}\ \boldsymbol{p}\ \text{の倍数でないと矛盾！}$$

となり、そういうことがないことがわかる——他の組み合せでも同様である．

もう 1 つ「 重要な事実 」を確認しておく．それは

「 $\boldsymbol{x,\ y}$ **のうち、一方は偶数で他方は奇数である** 」

ということだが、これはすでに述べた．その結果、トウゼン $\boldsymbol{z}$ **は奇数**である．

まずは、以上のことがらを上記の 11 例で確認してもらいたい．その上で、3 数 $x,\ y,\ z$ を追いつめていく．そのために ① を変形しておこう．

すなわち

$$x^2=z^2-y^2=(z+y)(z-y) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ②$$

ここで、x を偶数とすると $y,\ z$ は奇数だから、$x,\ z+y,\ z-y$ はともに偶数になる．

そういうことなら ② の両辺を 4 で割ろう．

$$\left(\frac{x}{2}\right)^2=\underbrace{\left(\frac{z+y}{2}\right)}_{\text{整数 } m_1}\cdot\underbrace{\left(\frac{z-y}{2}\right)}_{\text{整数 } n_1}=m_1n_1 \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots ③$$

ここで、y と z が互いに素であるから、$\dfrac{z+y}{2}=m_1$ と $\dfrac{z-y}{2}=n_1$ は互いに素である．

そこで ③ だが、これは互いに素である 2 数 m_1 と n_1 との積 m_1n_1 が $(\text{整数})^2$ であることを意味している．このときは $m_1,\ n_1$ がともに $(\text{整数})^2$ の形であるということだ．

どうしてこういうことがいえるかというと、③ の左辺が $\dfrac{x}{2}$ が整数で

$$\left(\frac{x}{2}\right)^2=p_1^{2\alpha}p_2^{2\beta}\cdots\cdots p_k^{2\omega} \quad (p_1,\ p_2,\ \cdots,\ p_k\ \text{は異なる素数で、}\alpha,\ \beta,\ \cdots,\ \omega\text{は正整数})$$

で、たとえば素数 p_1 に注目すると、これは偶数個含まれている．

そうすると右辺の m_1n_1 にも p_1 は偶数個含まれる．しかも m_1と n_1 は互いに素であるから、そのどちらか一方に先の偶数個が全部ゴッソリと含まれることになり、これは、他の素因数 $p_2,\ p_3,\ \cdots,\ p_k$ についても同様だから m_1, n_1 のいずれも平方数になるわけである．

以上のことから

$$m_1 = m^2,\quad n_1 = n^2,\qquad m, n \text{ は互いに素！}$$

がいえて、$m > 0,\ n > 0$ として

$$\frac{z+y}{2} = m^2,\qquad \frac{z-y}{2} = n^2,\qquad \left(\frac{x}{2}\right)^2 = m^2n^2$$

$$\boldsymbol{x = 2mn,\qquad y = m^2 - n^2,\qquad z = m^2 + n^2}$$

となり、これは明らかに ① を満たしていて、これが**不定方程式** ① の**一般解**である———両辺に入れて確認せよ！

残る問題は、$x,\ y,\ z$ に 1 以外の正の公約数がないような m, n をどのようにとればよいか、ということだが、これは次の 3 条件を満たすように決めればよい．つまり

(1) $\boldsymbol{m,\ n}$ **は互いに素**　　**(2)** $\boldsymbol{m > n}$
(3) $\boldsymbol{m,\ n}$ **の一方が偶数で他方が奇数となるようにとる．**

とまとめられる．そして、これは明らかに ① を満たしている———これでやっと**準備完了**だ．

そうすると、問題の 3 辺の積は

$$\begin{aligned} P &= xyz \\ &= (2mn)\cdot(m^2 - n^2)\cdot(m^2 + n^2) \\ &= 2mn(m^4 - n^4) \end{aligned}$$

で、これが上記の (1)(2)(3) の条件の下で $60 = 4 \times 3 \times 5$ の倍数であることをいえばよい．そこで、まず「 P が 4 の倍数であること 」については

$$2mn \equiv 0 \pmod 4 \quad \longleftarrow \quad m, n \text{ の一方は偶数で他方は奇数！}$$

$$\therefore\ P \equiv 0 \pmod 4 \quad \longleftarrow \quad \boldsymbol{P} \text{ は } \mathbf{4} \text{ で割り切れる！}$$

次に「 P が 3 の倍数であること 」については

$m,\ n$ のどちらかが 3 の倍数のとき

$$m \equiv 0 \pmod 3,\ \text{または } n \equiv 0 \pmod 3$$

$$\therefore\ P \equiv 0 \pmod 3 \quad \longleftarrow \quad \boldsymbol{P} \text{ は } \mathbf{3} \text{ で割り切れる！}$$

だから、あとは「 $m,\ n$ のどちらも 3 の倍数でない場合 」をいえばよい．

この場合、m と 3、n と 3 はいずれも互いに素であるから、前掲の「 **フェルマーの小定理** 」に登場してもらう．すなわち．

任意の正整数 a と、任意の素数 p に対して
$\boldsymbol{a^{p-1} \equiv 1 \pmod p}$

これを用いると

$$m^{3-1} = m^2 \equiv 1 \pmod 3,\qquad n^{3-1} = n^2 \equiv 1 \pmod 3$$

$$\therefore\ m^2 - n^2 \equiv 0 \pmod 3 \qquad \therefore\ P \equiv 0 \pmod 3 \quad \longleftarrow \quad \boldsymbol{P} \text{ は } \mathbf{3} \text{ で割り切れる！}$$

最後に「 P が 5 の倍数であること 」についてだが、これは上記「 3 の場合 」と同様である．

改めて書くほどでもないが、念のため、「 ダメ押し 」をしておく．つまり、$m,\ n$ のどちらかが 5 の倍数のときは

$$m \equiv 0 \pmod 5,\ \text{または } n \equiv 0 \pmod 5$$

$$\therefore\ P \equiv 0 \pmod 5 \quad \longleftarrow \quad \boldsymbol{P} \text{ は } \mathbf{5} \text{ で割り切れる！}$$

だから、あとは「 $m,\ n$ が 5 の倍数でない場合 」をいえばよい．

m と 5、n と 5 はいずれも互いに素であるから、前掲の「 **フェルマーの小定理** 」より

$$m^{5-1} = m^4 \equiv 1 \pmod 5, \quad n^{5-1} = n^4 \equiv 1 \pmod 5$$

$$\therefore \quad m^4 - n^4 \equiv 0 \pmod 5 \qquad \therefore \quad P \equiv 0 \pmod 5 \ \longleftarrow \ \boldsymbol{P} \text{ は } \mathbf{5} \text{ で割り切れる！}$$

結局、 $P \equiv 0 \pmod{60}$ がいえて、条件は証明された.

＜ end. ＞

1.3　素数と素因数分解、他

1.3.1　素数と合成数

1.3.1.1　素数

すべての**自然数**は、まず最小単位の 1 があって、その 1 に次々に 1 を加えていくと得られるから、「たし算」を基準に考えると 1 というその最小単位からできているかに見えるが、「かけ算」を基準に考えるとそうはいかない———もっとちがった見方もある．

つまり、自然数をなるべく小さい数の積に分けていくと、一般には

$$6 = 2 \times 3, \quad 21 = 3 \times 7, \quad 50 = 2 \times 5^2$$

などのように、これ以上細かく分けられないところまで分解した積の形で表すことができる．ところが

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ \cdots\cdots\cdots\cdots$$

などは、それ以上細かく分解することができない．このような数を**素数**というのである．

まず、この**素数**の然るべき定義からハナシを始めよう．

素数の定義

1 より大きい整数で、1 とそれ自身以外に正の約数をもたない整数を**素数**という．

これに対して、上記の 6, 21, 50 のような数は 1 とそれ自身以外にも正の約数をもっている．つまり、自然数の中には 1 でも素数でもない数が存在する．そのような数を**合成数**という．

すなわち、自然数はその約数の個数に注目すると

$$\text{自然数}\begin{cases} \text{正の約数が 1 つ} \cdots\cdots\cdots\cdots\cdots\cdots\cdots 1 \\ \text{正の約数が 2 つ} \cdots\cdots\cdots\cdots\cdots\cdots\cdots \text{素数} \\ \text{正の約数が 3 つ以上} \cdots\cdots\cdots\cdots\cdots\cdots \text{合成数} \end{cases}$$

と分類される．

＜メモ＞

■ エラトステネスの篩 (ふるい)——— 素数を探す方法

素数を求めるにはどうすればよいか———**エラトステネスの篩 (ふるい)** が有名である．エラトステネス (BC.275〜194) は古代ギリシャの数学者といわれているから、はるかなはるかな昔から人々はこのテーマに興味を持っていたようである．

これは、素数の倍数の配列規則を利用したもので、なかなかおもしろい———以下、古代ギリシャを堪能してもらいたい．

まず、自然数を大きさの順に並べておく．そうすると

(i) 2 の倍数は 2 から始まり 1 つおきに並ぶ．

$$1,\ \mathbf{2},\ 3,\ \mathbf{4},\ 5,\ \mathbf{6},\ 7,\ \mathbf{8},\ 9,\ \mathbf{10},\ \cdots\cdots\cdots\cdots\cdots$$

(ii) 3 の倍数は 3 から始まり 2 つおきに並ぶ．

$$1,\ 2,\ \mathbf{3},\ 4,\ 5,\ \mathbf{6},\ 7,\ 8,\ \mathbf{9},\ 10,\ \cdots\cdots\cdots\cdots\cdots$$

(iii) 一般に、素数 p の倍数は p から始まり $(p-1)$ 個おきに並ぶ．

$$\underbrace{1,\ 2,\ \cdots}_{(p-1)\text{ 個}},\ \boldsymbol{p},\ \underbrace{\cdots\cdots}_{(p-1)\text{ 個}},\ \boldsymbol{2p},\ \underbrace{\cdots\cdots}_{(p-1)\text{ 個}},\ \boldsymbol{3p},\ \cdots\cdots\cdots\cdots\cdots$$

とりあえず、ここまでの状況をシッカリ把握しておいてもらいたい．その上で次の操作をすることによって素数が求められるのである———これは実験だから、簡単のために 100 以下としておく．

1 を消す．
2 を残し、2 の倍数をすべて消す．
3 を残し、3 の倍数をすべて消す．
5 を残し、5 の倍数をすべて消す．
7 を残し、7 の倍数をすべて消す．

このようにして残った 25 個が 100 以下のすべての素数である．すなわち

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,$$
$$53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97$$

である———しかし、本当にこれでよいのか．

上記だけでは、素数が 7 のときまでしかやっていないではないか、という疑問が残る．しかし、結論を言うとそれでよい．

それは、次の定理で約束されているからである———興味深いハナシだから触れておく．

定理

自然数 N が $\sqrt{N}$ $(N>1)$ を越えない素数で割り切れないならば N は素数である．

(証明) これはマトモには攻めにくい———**対偶をとる**．すなわち

対偶： $\boldsymbol{N}$ が素数でないならば、$\boldsymbol{N}$ は$\boldsymbol{\sqrt{N}}$を越えない素数で割り切れる．

を示せばよい．

つまり、N は 1 でないから、素数でなければ合成数である．そこで N は 1 でない 2 つの自然数 $a,\ b$ を用いて

$$\boldsymbol{N=ab}\quad (a \leqq b)$$

とおくことができる．

このとき $\boldsymbol{\sqrt{N}<a}$ とすると

$$\sqrt{N}<a \leqq b \qquad \therefore\ \ N<a^2 \leqq ab=N \qquad \therefore\ \ N<N$$

となり**不合理**である．よって $a \leqq \sqrt{N}$ でなくてはならない．

したがって、$\sqrt{N}$ は $\sqrt{N}$ 以下の因数 a をもち、a が素数ならすでに条件を満たしており、a が合成数なら N は a より小さい素数で割り切れる———デキタ．すなわち、定理は証明された．

この定理を上記に適用すると、100 以下の素数を調べるのだから $\sqrt{100}=10$ 以下の素数、すなわち 2, 3, 5, 7 を調べればよい、ということになる．

■ ユークリッドの素数定理———素数は無限に存在する

前掲の例で 100 以下の素数については調べたが、100 より大きい素数はどうなっているのだろうか．この疑問に答えるのが次の定理である———**背理法**を用いた巧妙な証明がユークリッドの「 幾何学原本 」に載っているので、以下に解説しておこう．

ユークリッドの素数定理

素数は無限に存在する．

(**証明**) **背理法**で証明する———素数が有限個 (n 個) であると仮定して、それが不合理であることをいえばよい．

有限個 (n 個) の素数だから、それを小さい順に並べて番号をつける．すなわち

$$p_1,\ p_2,\ \cdots\cdots\cdots,\ p_n \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

とすることができる．

そして、これらの積より 1 だけ大きい自然数 N を作ると

$$N=(p_1p_2\cdots\cdots\cdots p_n)+1 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ②$$

であるが、これトウゼン 1 より大きいから、N は素数か合成数かのいずれかである．

N が**素数**であるとすると、これは ① の n 個の素数のどれよりも大きいので、素数の個数が n より大きくなって仮定に矛盾する．

N が**合成数**であるとすると、N は少なくとも 1 つの素因数をもつことになる．それを ① のどれか、つまり p_k ($k=1,\ 2,\ \cdots,\ n$ のどれか) とすると、② より N は p_k で割ると 1 余って割り切れないので p_k が N の素因数であることに矛盾する．

そういう訳で、結局、素数の個数は**無限個**でなくてはならない、ということになって証明を終わるのである．

★ いろいろある

最近は整数論に**解析的手法**も導入され、この定理のいろいろな証明方法も開発されているが、われわれとしては、このあたりが現段階での**守備領域の限界**というところであろう．

しかし、まだ未解決のものがヤマのようにあり、それらにひたすら立ち向かった先人たちがいたという事実は、私たちに日常とはちがった角度から新しい**夢**と**勇気**を与えてくれるような気もしないではない．

＜ end. ＞

■ 「 素数 」を探すロマン

大体、整数論とは何か．ここで、整数を研究する学問などと言っても始まらない———簡単にいうと、これは「 素数を調べる学問である 」と言ってよい．

したがって、古くから数学者は「 素数を求める方法 」について、情熱的にいろいろな試行錯誤を繰り返して来たのである．興味深いので、ここに 2 つばかり例をあげておく．

- **メルセンヌ素数**

これは

$$\boldsymbol{M_p = 2^p - 1} \ \ \textbf{(ただし、}\boldsymbol{p}\textbf{ は素数)}$$

の形をした素数のことで、フランスの修道僧**マラン・メルセンヌ** (1588〜1648) の名前をとって名づけたものである．この計算を実行すると

$$M_2 = 2^2 - 1, \quad M_3 = 2^3 - 1, \ M_5 = 2^5 - 1, \quad M_7 = 2^7 - 1$$

までは確かに素数だが、$p = 11$ のときは

$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$$

で、これは素数ではない———ここで、はかなく夢は破れてしまう．

それに、このタイプの数が素数か合成数かを見分けるには、p の値に 1 つ 1 つ素数を代入して計算しなければならず、それにこれらの数は急速に大きくなっていくので、その作業はかなり大変なものになる．

しかし、M_p が素数であるかどうかを見分ける非常に有効な方法も見つかり、コンピューターを使って相当大きな数まで発見されている．

現在知られている最大の**メルセンヌ素数**は M_{11213} で、その桁数は 3376 桁であると言われている———”言われている”というワケは筆者のパソコンの技術ではまだ無理ということです．そのうち、きっとそういうソフトにめぐり合うこともあるでしょう．

- **フェルマー素数**

これは

$$\boldsymbol{F_n = 2^m + 1} \ \ \textbf{(ただし、}\boldsymbol{m = 2^n}\textbf{)}$$

の形のもので、**フェルマー**によって導入された．フェルマーは

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

の 5 つの素数については計算したが、そのあとはやっていない．しかし、彼はこの種の数はすべて素数である、と信じていたようである．

ところが、オイラーが $n = 5$ の場合を計算して

$$F_5 = 4294967297 = 641 \times 6700417$$

となり、F_5 が素数でないことを示してしまった．

コンピューターを使った計算でも、$n \geqq 5$ のときの素数はまだ 1 つも発見されておらず、上記の 5 個以外にはこの形の素数は存在しないのではないか、と考えられるようになってきている．まあ、いずれにしても、まだまだわからないことがたくさんある ということである．

■ 改めて、「 素数 」とは何か———例題で確認する

＜ 例 1 ＞

x を整数とするとき、次の (1) (2) が素数となるような x を求めよ．

(1) $x^4 + 4$　　(2) $x^4 - 6x^2 + 25$

(解) (1) 素数は「 1 と自分自身以外に約数をもたない数 」ことであるから、まず、与えられた $\boldsymbol{x^4 + 4}$ が「 **積のカタチに変形できるか** 」ということ———**デキル！**

しかし、ちょっと難しい———**チエ**が必要だ．つまり

$$\begin{aligned} x^4 + 4 &= x^4 + 4 + 4x^2 - 4x^2 = x^4 + 4x^2 + 4 - 4x^2 \\ &= (x^2 + 2)^2 - (2x)^2 \quad \longleftarrow \quad A^2 - B^2 = (A + B)(A - B) \\ &= (x^2 + 2x + 2)(x^2 - 2x + 2) \ \longleftarrow \ x^2 \pm 2x + 2 = (x \pm 1)^2 + 1 > 0 \end{aligned}$$

ゆえに $x^2 + 2x + 2 = 1$, または $x^2 - 2x + 2 = 1$ だが

$$x^2 + 2x + 2 = 1 \ \longrightarrow \ (x + 1)^2 = 0 \qquad \therefore \ \ x = -1$$

$$x^2 - 2x + 2 = 1 \ \longrightarrow \ (x - 1)^2 = 0 \qquad \therefore \ \ x = 1$$

そこで、x の値に ± 1 を入れてそれぞれの因数とその積の結果を調べると

x	-1	1
x^2+2x+2	1	5
x^2-2x+2	5	1

$\therefore\ \ x^4+1=1\times 5=5\times 1=5 \longleftarrow$ **確かに素数！**

で、求める x の値は $x=\pm 1$ であることがわかる．

(2) 考え方は (1) と同様である．

$$\begin{aligned} x^4-6x^2+25 &= (x^4+10x^2+25)-16x^2 \\ &= (x^2+5)^2-(4x)^2 \quad \longleftarrow\ A^2-B^2=(A+B)(A-B) \\ &= (x^2+4x+5)(x^2-4x+5) \ \longleftarrow\ x^2\pm 4x+5=(x\pm 2)^2+1>0 \end{aligned}$$

ここで

x	-2	2
x^2+4x+5	1	17
x^2-4x+5	17	1

$\therefore\ \ x^4-6x^2+25=1\times 17=17\times 1=17$

x^4-6x^2+25 は確かに素数となり、求める x の値は $x=\pm 2$ である．

★ **因数分解が難しい．**

(1) では x^4+1、 (2) では x^4-6x^2+25 の因数分解が難しい．結果を言われればそうだが、いきなり出されるとパニクルのではないか———用心、用心！

＜ end. ＞

＜ 例 **3** ＞

等式 $p=2^q-1$ において、q は正の整数とする．

(1) $q=4$ のとき p が素数でないことを示せ．

(2) p が素数ならば、q も素数であることを証明せよ．

(解) (1) $q=4$ のときは

$$p=2^4-1=(2^2+1)(2^2-1)=\mathbf{5\times 3}=15 \longleftarrow \text{合成数！}$$

(2) 「 素数である 」ことを示すのはやりにくい———**対偶**をとる．つまり

$$\boldsymbol{q}\ \text{が合成数} \implies \boldsymbol{p}\ \text{も合成数}$$

を示せばよい．そこで、q が合成数ならば、$m,\ n$ を 1 と異なる正整数として、$q=mn$ とおくことができるから

$$\begin{aligned} p &= 2^q-1=2^{mn}-1=(2^m)^n-1 \\ &= (2^m-1)\{2^{m(n-1)}+2^{m(n-2)}+\cdots\cdots+2^m+1\} \ \longleftarrow\ \text{因数分解！} \end{aligned}$$

右辺の 2 つのカッコ内はいずれも 1 より大きい整数であるから、**右辺は合成数**である．

ゆえに、q が素数であることが証明された．

★ **ただし、(2) の逆は成り立たない．**

たとえば、$q=11$ (素数) などとすると

$$2^{11}-1=2047=23\times 89 \longleftarrow \text{これは素数ではない！}$$

のような反例を容易に探すことができる．

＜ end. ＞

＜例 **4**＞

「 3 と 5 」「 41 と 43 」のように、p と $p+2$ とがともに素数であるとき、この 1 対の素数を**双児素数**という.
「 3 と 5 」の場合を除き、双児素数にはさまれた自然数は 6 の倍数であることを示せ.

(解) すべての自然数は m を負でない整数として

$$6m-2,\ 6m-1,\ 6m,\ 6m+1,\ 6m+2,\ 6m+3$$

のどれかで表されるが、この中で素数になり得るものは $6m \pm 1$ だけである.

(i) $p = 6m-1$ のとき、$p+2 = 6m+1$ で、この 2 数にはさまれる自然数は $6m$ のみ.
(ii) $p = 6m+1$ のとき、$p+2 = 6m+3$ で、これは素数にはなりえない.

以上の考察から、条件を満たすものは (i) の場合で、それは $p = 6m-1$ のときである.

★ 「 双児素数 」は無限にあるか.

実は、**双児素数**が無限にあるかどうかは、まだわかっていない. 素数にはいろいろな話題があり、話題そのものは誰もがわかる程度に易しいものが多いが、その証明となると意外に難しく、いまだに解決されていないものが多いのである.

＜ end. ＞

1.3.1.2　素因数分解

ここで素数に関する重要な定理をあげておく．

素因数分解の「 可能性 」と「 一意性 」

(1) すべての自然数は素数の積の形で表される．
(2) また、その表し方は因数の順序のちがいを除けばただ 1 通りである．

(解説) (1) (2) これらの定理の主張するところは、たとえば

$$24 = 2^3 \cdot 3, \quad 252 = 2^2 \cdot 3^2 \cdot 7$$

のような分解についてのハナシである．先の例でいえば

$$24 = 2^3 \cdot 3 = 3 \cdot 2^3$$

のように、分解の順序の違いを無視すれば、その分解の仕方はただ 1 通りしかない、ということである．このことは上記の例の場合は、経験的にほとんど自明である．

それなら、「 そんな当たり前のことをナンデ？ 」と思うかも知れないが、たとえば**ガウスの整数**とよばれている

$$a + bi \quad (a,\ b \text{ は整数})$$

などのように、整数の概念を拡張すると、タダの「 整数 」のときのように単純にただ 1 通り (一意性) というわけにはいかなくなることが起こる．

そういう事情から、上記の表現は、われわれの守備領域である「 **整数** 」**のもつ固有の属性**をえぐり出して**区別**している、と考えればよい——まあ、**自明**としてよかろう．

一般に、自然数 a を

$$a = p^\alpha q^\beta r^\gamma \cdots\cdots \ (\ 1 < p < q < r < \cdots\cdots)$$
$$\longleftarrow \ p,\ q,\ r \cdots\cdots \text{ は素数、} \alpha,\ \beta,\ \gamma,\ \cdots\cdots \text{ は 0 または正整数！}$$

と表したものを、a の**素因数分解の標準形**、または**標準分解**という．

＜ end. ＞

(注) **1 は素数ではない——素因数分解の一意性に関係**

1 は、1 とそれ自身以外に正の約数をもたない、という制約だから 1 も素数の仲間に入れてもよさそうなものだが、これは除かれている．

そのワケは、もし 1 を素数とすると、たとえば

$$6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1^3 \cdot 2 \cdot 3 = \cdots\cdots\cdots\cdots$$

のように、素因数分解の**一意性**が崩れてしまう．つまり、上記の定理が成り立たないので、整数論の組み立てが根本から壊れてしまう．そういう事情で 1 は素数から除かれている——これは**この定理の重要性**とあわせて知っておいてもよいことがらである．

(注) ＜ end ＞

＜メモ＞

■ 改めて、素因数分解

素因数分解については、素数のところでも出てきたし、随所にあらわれてその都度、使い方などに触れてきたから、いまさら改めて説明でもあるまい．ここでは例題を 1 つあげるにとどめる．

＜ 例 ＞

自然数 n $(n \geqq 2)$ が、k 個の異なる素数で割り切れ、それ以外に素因数をもたないとき

$$\log n \geqq k \log 2$$

であることを証明せよ．

(解)　n が k 個の異なる素数　$p_1,\ p_2,\ \cdots\cdots,\ p_k$　で割り切れるものとする．そうすると、$a,\ b,\ \cdots\cdots,\ m$　を正整数として

$$n = p_1^a p_2^b \cdots\cdots p_k^m \quad \text{ただし、} p_1,\ p_2,\ \cdots\cdots,\ p_k \text{は素数とする．}$$

とおくことができる．

ここで $p_1,\ p_2,\ \cdots\cdots,\ p_k$ は素数であるから、いずれも 2 以上である．したがって

$$n = p_1^a p_2^b \cdots\cdots p_k^m \geqq 2^a \cdot 2^b \cdots\cdots 2^m = 2^{a+b+\cdots\cdots+m} \cdots\cdots\cdots\cdots ①$$

ここで、 $a,\ b,\ \cdots\cdots,\ m$　は k 個の正整数だから

$$a + b + \cdots\cdots + m \geqq k$$

これを ① に適用すると

$$n \geqq 2^k \qquad \therefore \quad \log n \geqq \ \log 2^k = k \log 2$$

ゆえに、条件は証明された．

＜ end. ＞

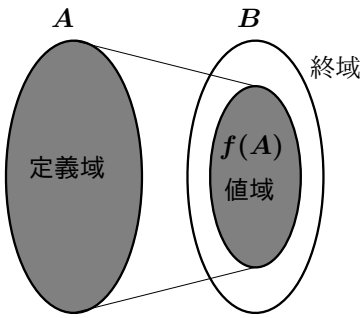
1.4　整数論的関数

ここでは、あえて**整数論的関数**などという、何やら難しい言葉を使ったが、いきなりこれでは困るだろう———少し説明をしてから本論に入ることにする.

まあ、字面でいえば整数論にかかわる関数を扱うのだが、まずはその**関数**という言葉の説明をしなくてはなるまい. それには、たとえば、関数 $f(x)$ が

$$f(x) = 2x + 1 \quad (= y) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

で与えられる、とはどういうことか.



雑駁な説明だが、① の $f(x)$ の f の意味していることは、その**定義域**内の**任意の要素**であるすべての x に対して

2 倍する、そして **1 を加える** $\longleftarrow$ $2x + 1$

という**操作**、あるいは**計算**を意味している.

そして、そのようにして得られた y のすべてで構成される集合が**値域**である.

もう少し詳しくいうと、**定義域** A に対して $f(A)$ を**値域**といい、一般的には $f(A)$ は、実数全体とか、整数全体とかで構成される**終域** B の部分集合、すなわち

$$f(A) \subseteqq B$$

となっている.

そして、集合 A から集合 B への関数が f であるとき

$$f: \quad A \to B$$

と表す———これが関数 f の定義である.

さて、改めて**整数論的関数**だが、集合 $A,\ B$ の**少なくとも一方が整数の集合**であるとき、関数 f を**整数論的関数**と呼ぶのである.

しかし、そうは言ってもそのような関数がたくさんあるわけでもなく、ここでは、数学の入り口でありながらシッカリとはとらえにくい「 **整数** 」の**全体像**を、なるべく整理してとらえるために手段とでも考えてもらえばよい.

以下、典型的な整数論的関数のいくつかについて解説する.

1.4.1　約数の個数とその総和

＜1＞ 約数の個数についての考察

自然数 a の正の約数の個数はトウゼン与えられた a の値で決まるから a の**関数**である——すでに**素因数分解**で説明したから問題はなかろう．

これを $T(a)$ で表すと、これは自然数 N から N への関数であるから、**整数論的関数**の 1 つである．たとえば、$a = 360$ とすると

$$a = 2^3 \cdot 3^2 \cdot 5^1$$

この正の約数は、3 つの集合

$$A = \{\ 1,\ 2,\ 2^2,\ 2^3\ \},\quad B = \{\ 1,\ 3,\ 3^2\ \},\quad C = \{\ 1,\ 5^1\ \}$$

からそれぞれ 1 つの要素をとり、それらの積を作ることにとって得ることができる．したがって、a の正の約数の個数 $T(a)$ は

$$T(a) = (1+3)(1+2)(1+1) = 24$$

である——A から 4 通り、B から 3 通り、C から 2 通りのとり方と考えればよいから、これはごく当たり前のことだ！

一般に、自然数 a の**標準分解**を $\boldsymbol{a = p^\alpha q^\beta \cdots r^\gamma}$ とすると、その**約数**は

$$\boldsymbol{a = p^k q^l \cdots r^m}$$

の形で、$k,\ l,\ m$ のとり得る値は

$$\begin{array}{l} k = 0,\ 1,\ 2,\ \cdots\alpha \ \longleftarrow\ (1+\alpha)\text{ 通り} \\ l\ = 0,\ 1,\ 2,\ \cdots\beta \ \longleftarrow\ (1+\beta)\text{ 通り} \\ \quad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \quad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ m = 0,\ 1,\ 2,\ \cdots\gamma \ \longleftarrow\ (1+\gamma)\text{ 通り} \end{array}$$

だから、a の約数の個数 $T(a)$ は

$$\boldsymbol{T(a) = (1+\alpha)(1+\beta)\cdots\cdots(1+\gamma)\ \longleftarrow\ N\text{ から }N\text{ への関数！}}$$

つまり、整数の集合である定義域の**トビトビの要素** a に対して、関数 T によって、値域の**トビトビの要素**がそれぞれ確定する——ここではそういう関数関係のことを言っているのである．

また、このハナシは次のようにも拡張される．

$$\boldsymbol{T(ab) = T(a)T(b)}$$

$a,\ b$ が互いに素であるとき、$T(ab) = T(a)T(b)$ が成り立つ．

(**証明**) 先行き、さして役に立つとも思えないが、知っておいてもジャマにはならない．

まず $a,\ b$ の**標準分解**を

$$a = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m},\quad b = q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}$$

とおくと、p_1〜p_m，q_1〜q_n はすべて素数であり、**a，b が互いに素**であるから集合

$$P = \{\ p_1,\ p_2,\ \cdots p_m\ \},\quad Q = \{\ q_1,\ q_2,\ \cdots q_n\ \}$$

の間には**共通の要素がない**．したがって

$$ab = (\ p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}\ )\ (\ q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}\ )$$

で、その約数の個数は

$$\begin{aligned} T(ab) &= \{\ (1+a_1)(1+a_2)\cdots(1+a_m)\ \}\ \{\ (1+b_1)(1+b_2)\cdots(1+b_n)\ \} \\ &= T(a)T(b) \end{aligned}$$

である——こんなところでよろしいか．

＜end.＞

＜2＞ 約数の総和

いま、次のような式展開に注目してもらいたい．すなわち

$$\underbrace{(1+p+p^2+\cdots+p^{\alpha})}_{A}\underbrace{(1+q+q^2+\cdots+q^{\beta})}_{B}\cdots\cdots\underbrace{(1+r+r^2+\cdots+r^{\gamma})}_{C}$$

を展開する基本にもどって考える．

つまり、上記の**展開**で得られる**各項**は、因数になっている $A, B, \cdots,\ C$ から 1 つずつ項をとってかけ合わせた積として得られ、その一般項は

$$p^k q^l r^m \quad (\ k=0,\ 1,\ 2,\cdots,\alpha, \quad l=0,\ 1,\ 2,\cdots\beta, \quad m=0,\ 1,\ 2,\cdots,\gamma\ )$$

である．そして、それらの総和として上記の計算結果が求める $S(a)$ になることは、改めて説明するまでもない．

したがって、前掲の $T(a)$ は、この一般項の個数であるが、これは因数 $A, B, \cdots,\ C$ から 1 つずつ項をとるとり方の個数だから、それぞれの場合を $(1+\alpha)$ 通り、$(1+\beta)$ 通り, $\cdots\cdots,\ (1+\gamma)$ 通り と考えて

$$T(a) = (1+\alpha)(1+\beta)\cdots\cdots(1+\gamma)$$

としてもよい——式展開の基本である．

さて、ハナシを $S(a)$ にもどすと、求める $S(a)$ は上記の展開式そのものだから、各因数が等比数列の和になっていることに着目する．すなわち

$$\begin{aligned} \boldsymbol{S(a)} &= (1+p+p^2+\cdots+p^{\alpha})(1+q+q^2+\cdots+q^{\beta})\cdots(1+r+r^2+\cdots+r^{\gamma}) \\ &= \boldsymbol{\frac{1-p^{\alpha+1}}{1-p}\cdot\frac{1-q^{\beta+1}}{1-q}\cdots\frac{1-r^{\gamma+1}}{1-r}} \end{aligned}$$

として求められる——このあたりは入試の素材になりそうな気がするがどうだろう．

ともあれ、ここでも整数の集合である定義域の**トビトビの要素** a に対して、関数 S によって、値域の**トビトビの要素**がそれぞれ確定する——ここでは、そういう関数関係をテーマにしているわけである．

＜メモ＞

■ 正の約数の個数とその和

こういうテーマはいきなりくると弱いようだ———具体的な数値の問題でやっておく．

＜ 例 1 ＞

3312 と 4464 の正の公約数は全部でいくつあるか．また、それらの和を求めよ

(解) 3312 と 4464 の公約数のすべては、この 2 数の最大公約数の約数であるから、まず 2 数の最大公約数を求める．2 数をそれぞれ素因数分解すると

$$3312 = 2^4 \cdot 3^2 \cdot 23, \qquad 4464 = 2^4 \cdot 3^2 \cdot 31$$

であるから、最大公約数は $2^4 \cdot 3^2$ である．

ゆえに、2 数の正の公約数の個数は

$$(1+4)(1+2) = 15 \text{ (個)}$$

であり、それらの総和は

$$\begin{aligned}(1+2+2^2+2^3+2^4)(1+3+3^2) &= \frac{2^5-1}{2-1} \cdot \frac{3^3-1}{3-1} \\ &= 403\end{aligned}$$

である．

＜ end. ＞

＜ 例 2 ＞

6 の約数は 1, 2, 3, 6 で、それらの和は 6 の 2 倍になっている．このように、正の約数の和がもとの自然数の 2 倍になっているとき、その自然数を**完全数**という．

$p,\ q,\ r,\ s,\ t,\ u$ を素数として

(1) pq という形の完全数は 6 だけであることを示せ．

(2) $r^2 s$ という形の完全数はあるか．あればそれを求めよ．

(3) $t^2 u^2$ という形の完全数はあるか．あればそれを求めよ．

(解) (1) $p,\ q$ は素数であるから、pq の正の約数の和が $2pq$ になるためには

$$(1+p)(1+q) = 2pq \qquad \therefore\ \ pq - p - q = 1 \qquad \therefore\ \ (p-1)(q-1) = 2$$

ここで $p > q$ とすると

$$\begin{cases} p-1 = 2 \\ q-1 = 1 \end{cases} \qquad \therefore\ \ \begin{cases} p = 3 \\ q = 2 \end{cases} \qquad \therefore\ \ pq = 6$$

で、条件を満たすものはこれしかない．

(2) 同様に考えて

$$(1+r+r^2)(1+s) = 2r^2 s \qquad \therefore\ \ (r^2-r-1)s = r^2+r+1$$

ここで $r \geqq 2$ で

$$r^2 - r - 1 = r(r-1) - 1 > 0$$

であるから

$$s = \frac{r^2+r+1}{r^2-r-1} \geqq 2 \quad \longleftarrow \quad s \text{ は素数だから } s \geqq 2$$

$$\therefore\ \ r^2+r+1 \geqq 2(r^2-r-1) \qquad \therefore\ \ r^2-3r-3 \leqq 0$$

$$\therefore\ \ \underbrace{\frac{3-\sqrt{21}}{2}}_{(-)} \leqq r \leqq \underbrace{\frac{3+\sqrt{21}}{2}}_{3.7\cdots\cdots} \qquad \therefore\ \ r = 2,\ \ 3$$

これらの r の値に対して、$r=2$ のとき $s=7$ だが $r=3$ のときは s の整数値はない．
　ゆえに、この形の完全数は

$$r^2 s = 2^2 \cdot 7 = 28$$

のみである．
(3) 同様にして

$$(1+t+t^2)(1+u+u^2) = 2t^2u^2 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

ここで

$$1+t+t^2 = t(t+1)+1 \longleftarrow \text{これは奇数！}$$

同ように $1+u+u^2$ も奇数であるから、$(*)$ の左辺は奇数、右辺は偶数となり、この形の完全数はない．

★ 完全数について

　古代ギリシャでは数に関する迷信、信仰のような神秘主義があったらしい．それは、数字をギリシャ文字で表していたからだという説があるが、その辺はよくわからない．
　とにかく、その数に対する神秘主義では、1 つの数の約数が特に重視され、その約数の総和が、その数自身に等しい数を最も理想的な数と考えていたようである——当時のギリシャ人はその数自身を約数とは考えなかったというから、これは問題文中の**完全数**のことである．
　完全数は 6, 28 の他に、496, 8128 などがあるが、知られているのはいずれも偶数で、奇数の完全数があるかどうかは、まだわかっていない．
　ここに、完全数についての定理を紹介しておく．それは

$2^{n+1}-1$ が素数ならば、$2^n(2^{n+1}-1)$ は完全数である

というもので、偶数の完全数はすべてこの形になることがわかっている——証明しておこう．
　$2^{n+1}-1$ は素数だから、その正の約数は 1 と $2^{n+1}-1$ それ自身しかない．そこで、$2^n(2^{n+1}-1)$ のすべての約数の総和は

$$\begin{aligned}(1+2+2^2+2^3+\cdots+2^n)\{1+(2^{n+1}-1)\} &= \frac{2^{n+1}-1}{2-1}\cdot 2^{n+1} \\ &= 2\cdot\boldsymbol{\{2^n(2^{n+1}-1)\}} \longleftarrow \textbf{もとの数の 2 倍になっている！}\end{aligned}$$

となり、$2^n(2^{n+1}-1)$ は完全数である——まあ、おもしろい結果ではある．

＜ end. ＞

1.4.2　オイラーの関数

自然数 a より小さい自然数のうち、**a と互いに素**であるものの個数は a の関数である．この関数を、**$\phi(a)$** で表し、**オイラーの関数**という．これは、言い方を変えると

$$\frac{1}{a},\ \frac{2}{a},\ \cdots\cdots,\ \frac{a-1}{a}$$

のうちの**既約分数の個数**ということもできる——当たり前のことだ．

たとえば、$\boldsymbol{a=10}$ の場合、10 より小さい自然数のうち、**10 と互いに素**であるものは

$$1,\ 3,\ 7,\ 9 \quad \longrightarrow \quad \boldsymbol{\phi(10)=4}$$

である．入試にメッタに出るものでもないが、定理として以下にまとめておく．

オイラーの関数

(1) p が素数のとき、$\phi(p^k)=p^k\left(1-\dfrac{1}{p}\right)$ である．

(2) $p,\ q$ が素数のとき、$x=p^l,\ y=q^m$ ならば、$\phi(xy)=\phi(x)\phi(y)$ が成り立つ．

(3) a の標準分解を $a=p^\alpha q^\beta\cdots r^\gamma$ とすると

$$\phi(a)=a\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\cdots\cdots\cdots\left(1-\frac{1}{r}\right)$$

が成り立つ．

(**解説**) 改めて眺めてみると、何やら**難しそう**で手がだせない．そういうときは、落ち着いて**式や文字の意味していること**をシッカリと把握することである——いつでも、すべてはここから始まるものだ、と覚悟を決めてもらいたい．

(1) それにしてもわかりにくい．とすれば、**具体的な数値**を入れて考える．

たとえば、なるべく簡単な数値として $p=2,\ k=3$ あたりでどうか．そうすると

$$p^k=2^3=8 \quad (\text{本文の自然数 } a)$$

で、8 より小さい自然数のうち、**8 と互いに素**であるものの場合である．

まず、全部を並べておいて 8 と 1 以外の公約数をもつものを消してみればよい．

$$1,\ \cancel{2},\ 3,\ \cancel{4},\ 5,\ \cancel{6},\ 7,\ (8) \quad \longrightarrow \quad \text{求めるものは } 1,\ 3,\ 5,\ 7\ (4\text{ 個}) \qquad \therefore\ \phi(8)=4$$

となる——ここで、何をやったのか．

上記では、1 から $7=2^3-1\ (=a-1)$ までの整数から 2 の倍数 (偶数) を除いたのである．要するに、これを一般の場合でやれ、ということだからそのまま書けばよい．

改めて、求めるものは、$\phi(p^k)$ は 1 から $p^k-1\ (=a-1)$ までのうち、p^k と互いに素であるもの、つまり p の倍数でないものの個数である．

だから、1 から p^k-1 までの合計 p^k-1 個の整数の個数から、その中に含まれる p の倍数の個数を引けばよい——p の倍数は全部を書き上げてみるとよくわかる．

そこで、「 p の倍数 」の集合 P は

$$P=\{\ p,\ 2p,\ \cdots,\ p^2,\ (p+1)p,\ \cdots,\ \underbrace{(\ p^{k-1}\cdot p\ )}_{a\text{ だから除く}}\} \quad \longleftarrow \quad (\ p^{k-1}-1\ )\text{ 個！}$$

ゆえに、求める $\phi(p^k)$ は

$$\boldsymbol{\phi(p^k)} = (p^k - 1) - (p^{k-1} - 1) = \boldsymbol{p^k\left(1 - \frac{1}{p}\right)} \quad \longleftarrow \quad \textbf{デキタ！}$$

最後に p^k をくくりだすところなど作為的だが、これで (2), (3) につながるのだ.

(2) これはちょっと複雑だ．そういうときは、改めて**論点を整理してみる**とよい.

それには、$xy = p^\alpha q^\beta = a$ とおいてみる——$\phi(a)$ は「**a より小さい自然数**」で、「**a と互いに素**」であるものの個数のことである．つまり、1 から $a-1$ までの $a-1$ 個の整数から p, または q の倍数 を除いたものの個数を求めている.

そこで、p, q の倍数の集合をそれぞれ P, Q とすると

$$P = \{\ p,\ 2p, \cdots\cdots,\ \underbrace{(\ p^{\alpha-1}q^\beta \cdot p\ )}_{a\ \text{だから除く}}\ \} \ \longleftarrow\ (\ p^{\alpha-1}q^\beta - 1\ )\ \text{個！}$$

$$Q = \{\ q,\ 2q, \cdots\cdots,\ \underbrace{(\ p^{\alpha}q^{\beta-1} \cdot q\ )}_{a\ \text{だから除く}}\ \} \ \longleftarrow\ (\ p^{\alpha}q^{\beta-1} - 1\ )\ \text{個！}$$

$$P \cap Q = \{\ pq,\ 2pq, \cdots\cdots,\ \underbrace{(\ p^{\alpha-1}q^{\beta-1} \cdot pq\ )}_{a\ \text{だから除く}}\ \} \ \longleftarrow\ (\ p^{\alpha-1}q^{\beta-1} - 1\ )\ \text{個！}$$

であるから、「p または q の倍数」の個数は

$$\begin{aligned}\boldsymbol{n(P \cup Q)} &= \boldsymbol{n(P) + n(Q) - n(P \cap Q)}\\ &= (\ p^{\alpha-1}q^\beta - 1\ ) + (\ p^\alpha q^{\beta-1} - 1) - (\ p^{\alpha-1}q^{\beta-1} - 1\ )\\ &= p^{\alpha-1}q^\beta + p^\alpha q^{\beta-1} - p^{\alpha-1}q^{\beta-1} - 1\end{aligned}$$

ゆえに、$\phi(a)$ は全体の整数の個数からこれを引いて

$$\begin{aligned}\boldsymbol{\phi(xy)} &= \phi(a) = (a-1) - n(P \cup Q)\\ &= (\ p^\alpha q^\beta - 1\ ) - (p^{\alpha-1}q^\beta + p^\alpha q^{\beta-1} - p^{\alpha-1}q^{\beta-1} - 1)\\ &= p^\alpha q^\beta - p^{\alpha-1}q^\beta - p^\alpha q^{\beta-1} + p^{\alpha-1}q^{\beta-1}\\ &= p^\alpha q^\beta\left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right)\\ &= p^\alpha\left(1 - \frac{1}{p}\right) \cdot q^\beta\left(1 - \frac{1}{q}\right) = \boldsymbol{\phi(x)\phi(y)} \ \longleftarrow\ (1)\ \text{を用いた！}\end{aligned}$$

となる——結構タイヘンだったが、ともあれ片付いた.

(3) (1), (2) の結果を $a = p^\alpha q^\beta \cdots\cdots r^\gamma$ にそのまま使えばよいではないか．すなわち

$$\begin{aligned}\boldsymbol{\phi(a)} &= \boldsymbol{\phi(p^\alpha q^\beta \cdots\cdots r^\gamma)} \ \longleftarrow\ \text{ここで (2) を使う！}\\ &= \boldsymbol{\phi(p^\alpha)\phi(q^\beta)\cdots\cdots\phi(q^\gamma)} \ \longleftarrow\ \text{それぞれに (1) を使う！}\\ &= p^\alpha\left(1 - \frac{1}{p}\right)q^\beta\left(1 - \frac{1}{q}\right)\cdots\cdots r^\gamma\left(1 - \frac{1}{r}\right)\\ &= \underbrace{p^\alpha q^\beta \cdots\cdots r^\gamma}_{a}\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\cdots\cdots\left(1 - \frac{1}{r}\right)\\ &= \boldsymbol{a\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\cdots\cdots\left(1 - \frac{1}{r}\right)}\end{aligned}$$

となって**一件落着**となった—— まあ、おもしろい結果ではある.

＜メモ＞

■ 入試とオイラーの関数

まあ、次の問題を見てもらおうか.

＜ 例 ＞

自然数 n と互いに素であって、n を超えない自然数の個数を $f(n)$ で表す．このとき、$p,\ q$ を異なる 2 つの素数として

$$f(pq) = (p-1)(q-1)$$

であることを証明せよ.

また、この等式を用いて、$f(pq) = 3p + q$ を満たす素数 $p,\ q$ を求めよ.

(解) 1 から pq までの自然数の総数は pq 個であるから、この中で pq と互いに素でないものを引けば、それが $f(pq)$ である.

pq と互いに素でない数は、p または q を因数としてもつ．そこで、pq を超えない自然数で

(i) p を因数としてもつものは

$$p,\ 2p,\ 3p,\ \cdots\cdots,\ (q-1)p,\ qp \quad \longleftarrow \quad q \text{ 個！}$$

(ii) q を因数としてもつものは

$$q,\ 2q,\ 3q,\ \cdots\cdots,\ (p-1)q,\ pq \quad \longleftarrow \quad p \text{ 個！}$$

で、この中で共通なものをさがさなくてはならない———まず、pq があることはすぐにわかるが、実はこれしかないのである.

たとえば、(i) の kp $(1 \leqq k \leqq q)$ と (ii) の lq $(1 \leqq l \leqq p)$ が共通であったとすると

$$kp = lq \quad \therefore \quad k = \frac{lq}{p}$$

$p,\ q$ は互いに素であるから、l は p の倍数でなくてはならない．ところが $1 \leqq l \leqq p$ だから、$l = p$ の他はないのである．したがって、$k = q$ となり、(i) (ii) に共通なものは pq 以外にないことがわかる．そこで

$$\begin{aligned} f(pq) &= pq - (p+q-1) \quad \longleftarrow \quad (\text{全体}) - \{n(P) + n(Q) - n(P \cap Q)\} \\ &= pq - p - q + 1 = (p-1)(q-1) \end{aligned}$$

次に、$f(pq) = 3p + q$ を満たす $p,\ q$ だが、この条件は

$$pq - p - q + 1 = 3p + q$$

$$\therefore \quad pq - 4p - 2q + 1 = 0 \qquad \therefore \quad (p-2)(q-4) = 7$$

ここで $p - 2$ は負になることはないので、左辺の 2 つの因数は正で

$p-2$	7	1
$q-4$	1	7

$\therefore$

p	9	3
q	5	11

すなわち、求める $p,\ q$ の組は $(p, q) = (9,\ 5),\ (3,\ 11)$ である.

★ オイラーの関数は難しい.

上記の問題は、まあ、「 ころあい 」でなかなかよくできていて好ましいが、このオイラーの関数をテーマにした問題は、ちょっと張り切るとやたらメンドウな問題になってしまう.

だから、ころあいの問題には入試でもなかなかお目にかかれない———本問のような問題でその趣旨を確認しておくとよい.

＜ end. ＞

1.4.3　ガウスの関数

x をカギカッコではさんだ記号 $[\,x\,]$ を**ガウス記号**といい、**x を超えない最大整数**を表す——これがガウス記号の**定義**である．すなわち k を整数として

$$[\,\boldsymbol{x}\,] = \boldsymbol{k} \quad \Longleftrightarrow \quad \boldsymbol{k} \leqq \boldsymbol{x} < \boldsymbol{k+1} \cdots\cdots\cdots\cdots ①$$

である．この定義にしたがえば

$$f(x) = [\,x\,]$$

は実数の集合 R から整数の集合 Z への関数であるから、これも**整数論的関数**の 1 つとみることができる——素因数分解とは直接には関係ないが、他の整数論的関数とあわせてここで解説する．

さて、① は何を意味するか——具体的な数値で説明するのがよさそうだ．つまり

$$\begin{array}{llll}
[\,1.2\,] = 1, & [\,1.5\,] = 1, & [\,1.8\,] = 1 & \cdots \longleftarrow \text{整数部分をとって 1} \\
[\,2.3\,] = 2, & [\,2.6\,] = 2, & [\,2.9\,] = 2 & \cdots \longleftarrow \text{整数部分をとって 2} \\
[\,3.1\,] = 3, & [\,3.4\,] = 3, & [\,3.7\,] = 3 & \cdots \longleftarrow \text{整数部分をとって 3} \\
\cdots\cdots & \cdots\cdots & \cdots\cdots & \\
\cdots\cdots & \cdots\cdots & \cdots\cdots &
\end{array}$$

のように使うのであるが、慣れないとこれがなかなか難しい．改めて ① は

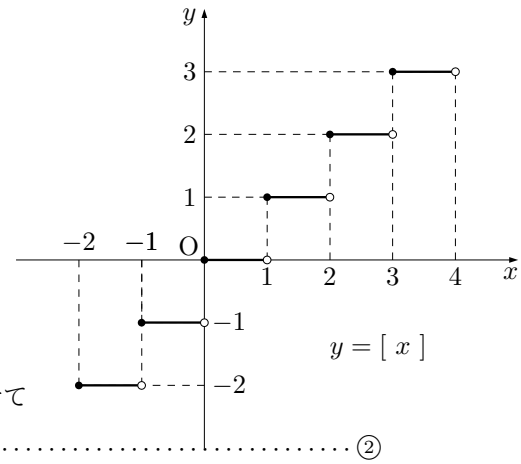
$$[\,x\,] \leqq x < [\,x\,] + 1$$

である．

実際の使い方については、改めて説明するが、その場合、右側の不等号から 1 を移項して

$$x - 1 < [\,x\,]$$

として使う場合が多い．



すなわち、① は左側の不等式とあわせて

$$\boldsymbol{x - 1 < [\,x\,] \leqq x} \cdots\cdots\cdots\cdots ②$$

だが、たとえば、$x \to \infty$ などのようにカンヅメ $[\,x\,]$ の中味の x を変化させたとしても、x が $[\quad]$ というカンにガードされているので、**カンヅメ丸ごと**である $[\,x\,]$ にはの直接の影響がない——② でいえばナマの x、つまり左側の $x-1$ と右側の x に作用するわけで、外側からしか見えない $[\,x\,]$ 全体がどうなるかはわからない．

そこで筆者は、**定義は ①、運用は ②** と説明することにしている．なお、この関係を xy 平面上に表したガウスの関数

$$y = [\,x\,]$$

のグラフは、上に示すように階段状の線分群で、それぞれの線分では**左の端**の点は入るが、**右の端**の点は除かれる．

(注) **ガウス記号 [$\boldsymbol{x}$] は「 切捨てそのもの 」ではない！**

ガウス記号 [$\boldsymbol{x}$] は、「 $\boldsymbol{x}$ を超えない最大整数 」のことだから、いかにも x の小数部分を切り捨てたかに見える．たとえば、本文で述べたように

$$[\ 2.302\ ] = 2, \quad [\ 0.15\ ] = 0$$

など、確かに x の小数部分を切捨てているが、だからといってガウス記号 [x] が切り捨ての関数と早合点してはならない．

実数の小数部分を切り捨てる操作も、やはり、実数の集合 R から整数の集合 Z への関数ではあるが、これは普通、「 $\boldsymbol{trunc(x)}$ 」で表され、[$\boldsymbol{x}$] とはちがうものである．

$x \geqq 0$ のときは、上記のように

$$[\ \boldsymbol{x}\ ] = trunc(x)$$

であるが、たとえば $trunc(-2.5) = -2$ で、[-2.5] は -2 ではなく -3 である．

これは、数直線上で見れば明らかで、-2.5 を超えない最大整数は -3 である．したがって、[x] と $trunc(x)$ との関係は

$$trunc(x) = \begin{cases} [\ x\ ] & (x \geqq 0) \\ [\ x\ ] + 1 & (x < 0) \end{cases}$$

となるのである．

しかし、この $trunc(x)$ という記号は高校数学には出てこないから心配しないでよい———ワケがわかればそれでよい．

なお、負の数の切り上げや四捨五入もあり得るが、筆者はこのトシになってもついぞ見かけたことがない———あまり実用的ではないのだと思う．

(注) ＜ end. ＞

＜メモ＞

■ ガウス記号を含む関数のグラフ

さて、ここでガウス記号 $[\ x\ ]$ を含む関数のグラフをいくつか描いてみよう――$[\ x\ ]$ の意味がいくらか具体的なカタチでつかめるかと思う．

＜ 例 ＞

次の関数のグラフを描け．ただし、x の範囲を $-2 \leqq x < 2$ とする．

(1) $y = x - [\ x\ ]$　(2) $y = [\ \frac{x}{3}\ ]$　(3) $y = x + [\ 2x\ ]$　(4) $y = x^2 - [\ x^2\ ]$

(解) (1) $y = x - [\ x\ ]$ のグラフ――x の範囲で場合を分けて考える．

(i) $-2 \leqq x < -1$ のとき：

$[\ x\ ] = -2 \quad \therefore\ \ y = x + 2$

(ii) $-1 \leqq x < 0$ のとき：

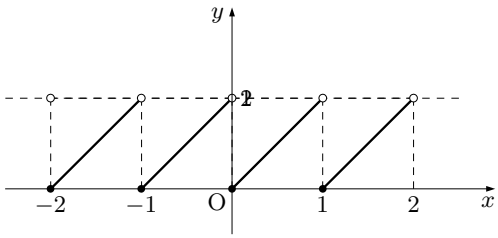
$[\ x\ ] = -1 \quad \therefore\ \ y = x + 1$

(iii) $0 \leqq x < 1$ のとき：

$[\ x\ ] = 0 \quad \therefore\ \ y = x$

(iv) $1 \leqq x < 2$ のとき：

$[\ x\ ] = 1 \quad \therefore\ \ y = x - 1$



$y = x - [\ x\ ]$

以上の考察から

$$y = \begin{cases} x + 2 & (-2 \leqq x < -1) \\ x + 1 & (-1 \leqq x < 0) \\ x & (0 \leqq x < 1) \\ x - 1 & (1 \leqq x < 2) \end{cases}$$

(2) $y = [\ \frac{x}{3}\ ]$ のグラフ．

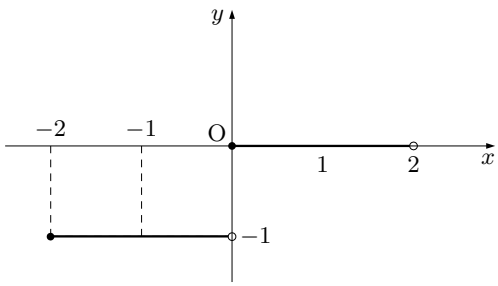
ガウス記号の中の $\frac{x}{3}$ に注目すると、$\boldsymbol{-\frac{2}{3} \leqq \frac{x}{3} < \frac{2}{3}}$ であるから

(i) $-\frac{2}{3} \leqq \frac{x}{3} < 0$ のとき：　$-2 \leqq x < 0$

$[\ \frac{x}{3}\ ] = -1 \quad \therefore\ \ y = -1$

(ii) $0 \leqq \frac{x}{3} < \frac{2}{3}$ のとき：　$0 \leqq x < 2$

$[\ \frac{x}{3}\ ] = 0 \quad \therefore\ \ y = 0$



$y = [\ \frac{x}{3}\ ]$

まとめると

$$y = \begin{cases} -1 & (-2 \leqq x < 0) \\ 0 & (0 \leqq x < 2) \end{cases}$$

(3) $y = x + [\ 2x\ ]$ のグラフ.

ガウス記号の中の $2x$ に注目すると $\boldsymbol{-4 \leqq 2x < 4}$ だから

(i) $-4 \leqq 2x < -3$ $(-2 \leqq x < -1.5)$ のとき

$[\ 2x\ ] = -4 \quad \therefore \quad y = x - 4$

(ii) $-3 \leqq 2x < -2$ $(-1.5 \leqq x < -1)$ のとき

$[\ 2x\ ] = -3 \quad \therefore \quad y = x - 3$

(iii) $-2 \leqq 2x < -1$ $(-1 \leqq x < -0.5)$ のとき

$[\ 2x\ ] = -2 \quad \therefore \quad y = x - 2$

(iv) $-1 \leqq 2x < 0$ $(-0.5 \leqq x < 0)$ のとき

$[\ 2x\ ] = -1 \quad \therefore \quad y = x - 1$

(v) $0 \leqq 2x < 1$ $(0 \leqq x < 0.5)$ のとき

$[\ 2x\ ] = 0 \quad \therefore \quad y = x$

(vi) $1 \leqq 2x < 2$ $(0.5 \leqq x < 1)$ のとき

$[\ 2x\ ] = 1 \quad \therefore \quad y = x + 1$

(vii) $2 \leqq 2x < 3$ $(1 \leqq x < 1.5)$ のとき

$[\ 2x\ ] = 2 \quad \therefore \quad y = x + 2$

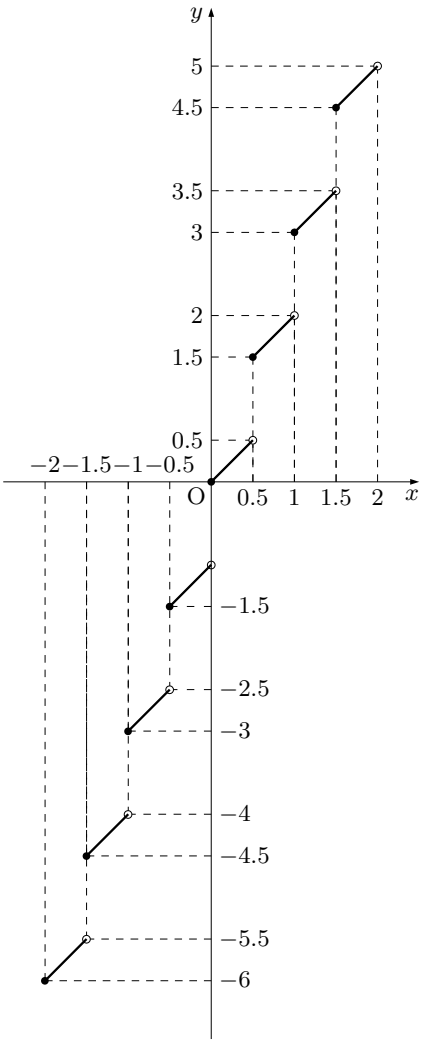
(viii) $3 \leqq 2x < 4$ $(1.5 \leqq x < 2)$ のとき

$[\ 2x\ ] = 3 \quad \therefore \quad y = x + 3$

以上まとめると

$$y = \begin{cases} x - 4 & (-2 \leqq x < -1.5) \\ x - 3 & (-1.5 \leqq x < -1) \\ x - 2 & (-1 \leqq x < -0.5) \\ x - 1 & (-0.5 \leqq x < 0) \\ x & (0 \leqq x < 0.5) \\ x + 1 & (0.5 \leqq x < 1) \\ x + 2 & (1 \leqq x < 1.5) \\ x + 3 & (1.5 \leqq x < 2) \end{cases}$$

となる———右図で確認せよ.

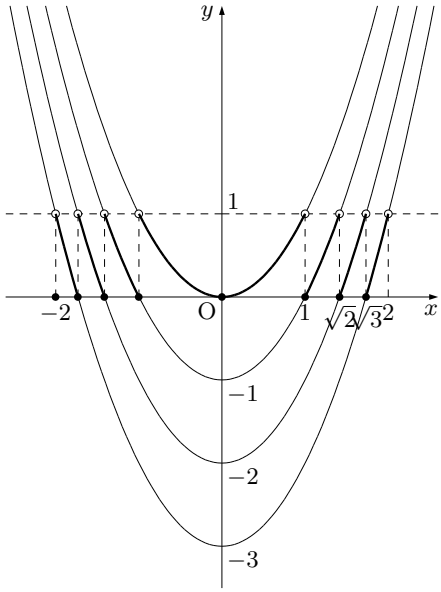


(4) $y = x^2 - [\ x^2\ ]$ のグラフ.

まず、ガウス記号の中の x^2 の範囲を求めると

$$-2 \leqq x < 2 \qquad \therefore\ \ \boldsymbol{0 \leqq x^2 < 4}$$

そこで、x^2 で場合を分けて考える.



(i) $0 \leqq x^2 < 1$ のときは、$0 \leqq |x| < 1$ で

$$[\ x^2\ ] = 0, \qquad \therefore\ \ y = x^2$$

(ii) $1 \leqq x^2 < 2$ のときは、$1 \leqq |x| < \sqrt{2}$ で

$$[\ x^2\ ] = 1, \qquad \therefore\ \ y = x^2 - 1$$

(iii) $2 \leqq x^2 < 3$ のときは、$\sqrt{2} \leqq |x| < \sqrt{3}$ で

$$[\ x^2\ ] = 2, \qquad \therefore\ \ y = x^2 - 2$$

(iv) $3 \leqq x^2 < 4$ のときは、$\sqrt{3} \leqq |x| < 2$ で

$$[\ x^2\ ] = 3, \qquad \therefore\ \ y = x^2 - 3$$

(v) $x = -2$ のときは

$$y = 2^2 - [\ (-2)^2\ ] = 4 - 4 = 0$$

以上まとめると

$$y = \begin{cases} x^2 & (0 \leqq |x| < 1) \\ x^2 - 1 & (1 \leqq |x| < \sqrt{2}) \\ x^2 - 2 & (\sqrt{2} \leqq |x| < \sqrt{3}) \\ x^2 - 3 & (\sqrt{3} \leqq |x| < 2) \\ 0 & (x = -2) \end{cases}$$

となって、図に示すグラフが得られる.

＜ end. ＞

■ ガウス関数 $[\,x\,]$ の実際

一応、まあ、キブンはわかったと思うが、慣れるまではなかなか難しい．ここで確認をかねて例題をあげておく．

＜例 1＞

次の方程式と不等式を解け．

(1) $\sqrt{x-[\,x\,]}+x=2$　　(2) $4\,[\,x\,]^2-36\,[\,x\,]+45<0$

(解) (1) 見かけは無理方程式だが、恐れずやってみよう．

まず、整理して見やすくすると

$$\sqrt{x-[\,x\,]}=2-x \cdots\cdots ①$$

だが、$[\,x\,]$ の性質から

$$\boldsymbol{[\,x\,]\leqq x<[\,x\,]+1} \quad \therefore\ 0\leqq x-[\,x\,]<1 \quad \therefore\ 0\leqq\sqrt{x-[\,x\,]}<1$$

このとき、これを ① の右辺に適用すると

$$0\leqq 2-x<1 \quad \therefore\ 1<x\leqq 2$$

そうすると

$$[\,x\,]=\begin{cases} 1 & (\longleftarrow\ 1<x<2 \text{ のとき}) \\ 2 & (\longleftarrow\ x=2 \text{ のとき}) \end{cases}$$

であるから、次のように場合を分けて考える．

(i) $1<x<2$ のとき

$$\boldsymbol{\sqrt{x-1}=2-x} \cdots\cdots ②$$

両辺は**負でない**から、2 乗して

$$\boldsymbol{x-1=(2-x)^2} \cdots\cdots ③$$

$$\therefore\ x^2-5x+5=0 \quad \therefore\ x=\frac{5\pm\sqrt{5}}{2} \ \longleftarrow\ \text{正号は②を満たさない！}$$

$$\therefore\ x=\frac{5-\sqrt{5}}{2}$$

(ii) $x=2$ のときは $[\,x\,]=2$ だから、① の両辺は 0 となって条件を満たす．

以上の考察から、求める解は　$2,\ \dfrac{5-\sqrt{5}}{2}$　である．

これでこの無理方程式は解けたわけだが、ここで 1 つ注意しておかねばならないことがある．それは「 $\boldsymbol{A=B}$ **ならば** $\boldsymbol{A^2=B^2}$ 」だが、この**逆は成り立たない**ということだ．

それは

$$A^2=B^2 \quad \therefore\ A=\pm B$$

つまり、2 乗したトタンに、$A=B$ の他に $A=-B$ も勝手に含まれてしまうという問題である．

上記でいえば、③ の中に

$$\sqrt{x-1}=-(2-x)$$

の解も含まれてしまう可能性が起こってくる．そこで「 正号は②を満たさない！」という**確認の証拠**が求められるのである――数学用語では**吟味** (ぎんみ) という．

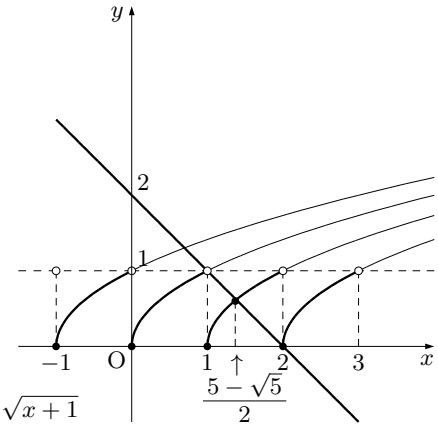
実数条件といい、**根号の規約**といい、**2 乗の同値性**といい、いろいろな「 **おさらい** 」のできるなかなかよい問題であった．

さて、方程式や不等式の問題はグラフを描くと視覚的にスッキリ見えるときがある———本問ではどうか．① の両辺を見て関数は

$$\begin{cases} y_1 = \sqrt{x - [\,x\,]} \ \cdots\cdots\cdots\cdots (*) \\ y_2 = 2 - x \ \cdots\cdots\cdots\cdots\cdots\cdots (**) \end{cases}$$

だが、$(*)$ では $x - [\,x\,]$ が x からその整数部分を引いたものだから $0 \leqq y_1 < 1$ だろう．

それに $(**)$ の y_2 の範囲をあわせて考えると、調べる x の範囲は「 0 から 3 くらいの間 」ということになろうが、それでも用心に $-1 \leqq x < 3$ くらいで考えてみるか．



$$\begin{aligned} -1 \leqq x < 0 \text{ のとき：} & [\,x\,] = -1 & \therefore\ y_1 = \sqrt{x+1} \\ 0 \leqq x < 1 \text{ のとき：} & [\,x\,] = 0 & \therefore\ y_1 = \sqrt{x} \\ 1 \leqq x < 2 \text{ のとき：} & [\,x\,] = 1 & \therefore\ y_1 = \sqrt{x-1} \\ 2 \leqq x < 3 \text{ のとき：} & [\,x\,] = 2 & \therefore\ y_1 = \sqrt{x-2} \end{aligned}$$

で、y_1 のグラフは図のように放物線の弧からできている．

これと直線 $y_2 = 2 - x$ は点 $(2, 0)$ で交わり、もう 1 つは $1 < x < 2$ の範囲に交点が 1 つあることがわかる．それが無理方程式を解いたときの

$$\sqrt{x-1} = 2 - x \ \longrightarrow\ x = \frac{5-\sqrt{5}}{2}$$

であることは説明するまでもない．

(2) $[\,x\,] = X$ とおいて、与えられた不等式の左辺を因数分解すると

$$4X^2 - 36X + 45 = (2X-3)(2X-15) < 0 \qquad \therefore\ 1.5 < X < 7.5$$

X は整数であるから

$$X = [\,x\,] = 2,\ 3,\ 4,\ 5,\ 6,\ 7$$

ここで

$$\begin{aligned} [\,x\,] = 2 &\ \longrightarrow\ 2 \leqq x < 3 \\ [\,x\,] = 3 &\ \longrightarrow\ 3 \leqq x < 4 \\ [\,x\,] = 4 &\ \longrightarrow\ 4 \leqq x < 5 \\ [\,x\,] = 5 &\ \longrightarrow\ 5 \leqq x < 6 \\ [\,x\,] = 6 &\ \longrightarrow\ 6 \leqq x < 7 \\ [\,x\,] = 7 &\ \longrightarrow\ 7 \leqq x < 8 \end{aligned}$$

これらの x の範囲はつながって、求める x の範囲は $2 \leqq x < 8$ である．

★ 無理方程式について

現行の高校の教科書で、**無理方程式**はグラフを描いて「 目見当で解を探す 」程度のことしか入っていない．筆者の個人的な意見としては、計算でキッチリと扱うべきであると思うが、如何ともしがたいところである．ここで詳しく解説するヒマはないが、要するに

(i) **実数条件** (ルート内 $\geqq 0$)　(ii) **根号の規約** $\sqrt{(\quad)} \geqq 0$

に条件を絞っておいて「 2 乗する 」のだが、わかりにくければ、ドンドン 2 乗して計算を進めて行って、求まった x(必要条件) のうち、2 乗する前の方程式を満たす (十分条件) ものだけを拾えばよい．

＜ end. ＞

＜例 **2**＞

(1) $100! = (2m-1) \times 2^n$ ($m,\ n$ は正の整数) とすると、n の値はいくらか.
(2) $100!$ の値を計算したとき、その末尾に 0 はいくつつくか.
(3) 同様に $1234!$ を計算したとき、その末尾に 0 はいくつつくか.

(解) 一見したところ、**ガウス関数**に関係のない問題に見える．実際、これは「 約数の個数の問題 」で、ガウスの関数とは直接には関係がないといってもよい.

まあ、そこのところは「 **今までの復習** 」だからシッカリとやってもらわなければならないが、その上で、改めてこの問題を「**ガウス関数との関連として**」ながめてもらいたい.

(1) まず、与えられた等式は何を意味するか．$(2m-1)$ は奇数だから 2 という因数はもたない．そこで $100!$ に 2 という素因数が何個含まれているかを調べればよい．それは、1 から 100 までの整数に、$2,\ 2^2,\ 2^3, 2^4,\ 2^5,\ 2^6$ の倍数がいくつあるかだが、それぞれ

$$50,\ 25,\ 12,\ 6,\ 3,\ 1\ (個)$$

であるから、$100!$ に含まれる 2 という素因数の個数は全部で

$$\mathbf{50+25+12+6+3+1} = 97\ (個) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ①$$

だから、$n = 97$ である.

だが、ちょっと説明すると、上記の 2 の倍数の個数 50 個には、すでに 2^2 の倍数も数えているから、ここで 2^2 の 1 つの因数 2 は数えてしまい、もう 1 つの因数 2 は 2^2 の個数 25 個のときに数えている のである.

つまり、① は 2 の次数の低いところで数えたものは順次除いて加えている のである――ここはなかなか難しいから注意してもらいたい.

(2) 末尾の 0 は $10 = 2 \times 5$ によって起こる.

だから、$100!$ に含まれる $10^k = 2^k \cdot 5^k$(k は正整数) を調べることになる．2^k については、すでに (1) で調べたから、5^k について調べる.

1 から 100 までの整数に含まれる $5,\ 5^2$ の倍数の個数は、それぞれ $20,\ 4$ であるから、$100!$ に含まれる 5 という素因数の個数は $20+4=24$(個) で、この個数の方が 2 という素因数の個数より少ないから、0 の個数はこの 5 の約数 24 個に制限される．つまり、0 は 24 個つく.

(3) (2) と同様に考える.

1 から 1234 までの整数に $5,\ 5^2,\ 5^3,\ 5^4$ の倍数はそれぞれ $246,\ 49,\ 9,\ 1$(個) ずつあるので、素因数 5 の総数は

$$246+49+9+1 = 305\ (個)$$

で、結局 $1234!$ の末尾には 0 が 305 個並ぶことになる.

★ ガウス関数による考察

素因数分解を前提にして、約数の個数を調べる方法としては次のような考え方がある．すなわち一般に、自然数 b が、a を自然数として a^n では割り切れるが、a^{n+1} では割り切れない とき

$$\boldsymbol{f_a(b) = n} \longleftarrow \text{意味は下の具体例とつき合わせて確認のこと！}$$

と書くことにする．たとえば、$24 = 2^3 \cdot 3$ だから

$$f_2(24) = 3 \longleftarrow 2^3\text{では割り切れるが}\ 2^4\text{では割り切れない！}$$
$$f_3(24) = 1 \longleftarrow 3^1\text{では割り切れるが}\ 3^2\text{では割り切れない！}$$
$$f_6(24) = 1 \longleftarrow 6^1\text{では割り切れるが}\ 6^2\text{では割り切れない！}$$

のようなアンバイの記号を導入する.

いま、p を素数とし、$[\ A\ ]$ を A を超えない最大整数とするとき

$$f_p(n!) = \left[\ \frac{n}{p}\ \right] + \left[\ \frac{n}{p^2}\ \right] + \left[\ \frac{n}{p^3}\ \right] + \cdots\cdots\cdots\cdots\cdots$$

$$\begin{array}{r|l} 2 & 100 \\ \hline 2 & 50 \\ \hline 2 & 25 \\ \hline 2 & 12 \\ \hline 2 & 6 \\ \hline 2 & 3 \\ \hline & 1 \end{array}$$

が成り立つ．本問でいうと

$$\begin{aligned} f_2(100!) &= \left[\ \frac{100}{2}\ \right] + \left[\ \frac{100}{2^2}\ \right] + \left[\ \frac{100}{2^3}\ \right] + \cdots\cdots\cdots\cdots\cdots \\ &= 50 + 25 + 12 + 6 + 3 + 1 \\ &= 97 \end{aligned}$$

となる———上記の ① と較べてみよ．

この計算を簡単にやるには、余りは無視して、右の計算をし、 50, 25, 12, 6, 3, 1 をとって加えればよいことがわかる．

また

$$\begin{array}{r|l} 5 & 100 \\ \hline 5 & 20 \\ \hline & 4 \end{array}$$

$$\begin{aligned} f_5(100!) &= \left[\ \frac{100}{5}\ \right] + \left[\ \frac{100}{5^2}\ \right] + \cdots\cdots\cdots\cdots\cdots \\ &= 20 + 4 = 24 \end{aligned}$$

も同様である．

ただし、 $\boldsymbol{f_p(n!)}$ で「 $\boldsymbol{p}$ **が素数**の場合に限る 」ことに注意しなければならない．しかし、そういうときは、たとえば $f_{10}(100!)$ のような場合には $10 = 2 \times 5$ と素因数分解して

$$f_{10}(100!) = \min\{f_2(100!),\ f_5(100!)\} \longleftarrow \text{大きくない方をとる！}$$

のようにして求めることになる———ともあれ、ハナシはずっと簡単になる．

＜ end. ＞

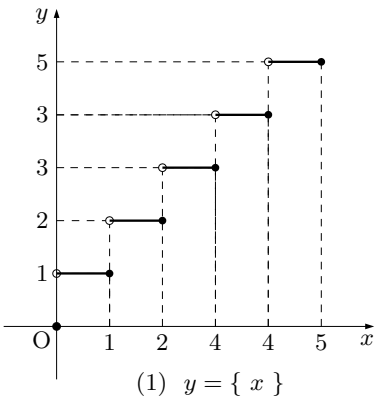
■ **ガウス関数の応用**

ガウス関数については、いろいろな応用面があるが、とりあえず手近の例では「 **切り上げ** 」、「 **切り捨て** 」と「 **四捨五入** 」が思いつく———以下に解説しておく．ただし、混乱を避けるために、とりあえず $\boldsymbol{x \geqq 0}$ としておく．

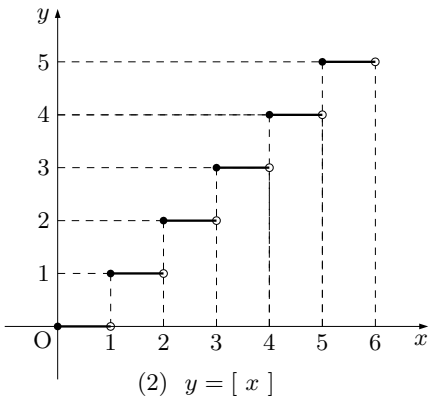
まず、「 **切り上げ** 」についてだが、x を切り上げて得られる整数を $\{x\}$ で表すと、これは x の関数として

$$y = \{x\}$$

である——— $y = [\ x\ ]$ のグラフと比較してみてもらいたい．



(1) $y = \{\ x\ \}$



(2) $y = [\ x\ ]$

この図で見ると、(1) の $y = \{x\}$ のグラフは、(2) の $y = [\ x\ ]$ のグラフを x 軸方向に (-1) だけ平行移動したカタチだが、少しちがっているところがある．

それは (1) ではそれぞれの区間の**左端**が除かれ、**右端**が含まれているが、(2) ではその逆になっている———グラフを見るポイントの 1 つ！

そうすると、x の 1 未満の部分を切り上げて得られる $\{x\}$ は

$$\{x\} = \begin{cases} [\ x+1\ ] & (x \neq [\ x\ ]) \\ [\ x\ ] & (x = [\ x\ ]) \end{cases}$$

となるのである．つまり、x が整数でなければ $\{x\} = [\ x+1\ ]$ である．

また、「 **切り捨て** 」は、$\boldsymbol{x \geqq 0}$ の場合はガウス関数 $[\ x\ ]$ そのものだから問題はなかろうが、実はおもしろい扱い方があるのでここに紹介しておく．

その利用というのはは、「 小数以下の切捨てに限らない 」ということ———こういうのが**知恵**というものだろう．

たとえば、4526 の 100 未満を切り捨てる場合は、$4526 \div 100 = 45.26$ としておいて、まずこの小数部分である 0.26 を切り捨て、そのあとで 100 倍すれば 4500 が得られるというものである．

これを一般化すれば、x の 10^n 未満を切り捨てるときは

$$\boldsymbol{\left[\ \frac{x}{10^n}\ \right] \times 10^n}$$

を計算すればよい．上記はこの式の $n = 2$ の場合、つまり

$$\left[\ \frac{4256}{10^2}\ \right] \times 10^2 = 4500$$

を実践したことがわかる．

次に「 **四捨五入** 」について考えてみよう．これには、新しい記号が必要だが、x を「 四捨五入 」して

$$\boldsymbol{y = (\ x\ )}$$

と表すことにする．

このグラフは右図 (3) のようになるが、これは (2) の $y = [\ x\ ]$ のグラフを x 軸方向に -0.5 だけ平行移動したものになっているので

$$y = [\ x + 0.5\ ]$$

のグラフである．したがって

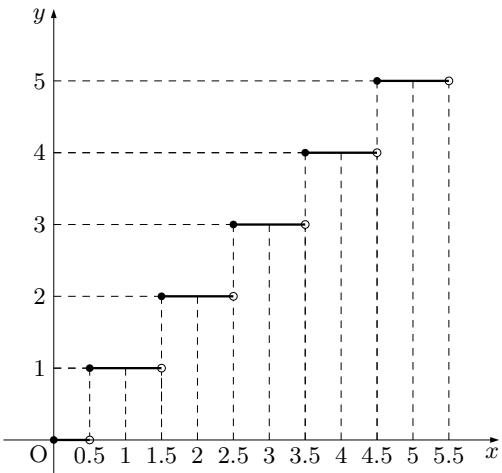
$$(\ x\ ) = [\ x + 0.5\ ]$$

となるが、「 **四捨五入** 」の基本原理が**可視的**に表現できて、なかなかおもしろい．

また、これも一般の場合、つまり、10^n 未満を 「 四捨五入 」するハナシに拡張することができる．すなわち

$$\boldsymbol{\left[\ \frac{x}{10^n} + 0.5\ \right] \times 10^n}$$

と表すことができる．



(3) $y = (\ x\ )$

■ **ガウス関数の重要な性質**

ガウス関数の性質をまとめておく．役に立つものもあるし、そうでもないがおもしろいものもある．**簡単な証明**をつけておくから、確認しておくべし．

1° $\boldsymbol{a}$ **を** $\boldsymbol{b}$ **で割った商を** $\boldsymbol{q}$ **とすると** $\boldsymbol{q = \left[\ \frac{a}{b}\ \right]}$、 **ただし** $\boldsymbol{a}$ **を整数、**$\boldsymbol{b}$ **を正整数とする．**

$$a = bq + r,\ \ 0 \leqq r < b \ \longrightarrow\ \frac{a}{b} = q + \frac{r}{b},\ \ 0 \leqq \frac{r}{b} < 1 \qquad \therefore\ \ [\ \frac{b}{a}\ ] = q$$

2° $[\,\boldsymbol{x+k}\,]=[\,\boldsymbol{x}\,]+\boldsymbol{k}$ **($\boldsymbol{k}$ は任意の整数)**

$[\,x\,]=n \;\longrightarrow\; n \leqq x < n+1$ (n は整数)

$\therefore\;\; n+k \leqq x+k < (n+k)+1 \qquad \therefore\;\; [\,x+k\,]=n+k=[\,x\,]+k$

3° $[\,\boldsymbol{x}\,] \leqq \boldsymbol{x} < [\,\boldsymbol{x}\,]+\boldsymbol{1}$

$n \leqq x < n+1$ (n は整数) のとき $[\,x\,]=n \;\longleftarrow$ 定義の通り！

$\therefore\;\; [\,x\,] \leqq x < [\,x\,]+1$

4° $\boldsymbol{x_1 < x_2 \implies [\,x_1\,] \leqq [\,x_2\,]}$

上記「 **3°** 」を用いると

$[\,x_1\,] \leqq x_1 < x_2 < [\,x_2\,]+1 \qquad \therefore\;\; [\,x_1\,] < [\,x_2\,]+1$

この両辺は整数だから

$[\,x_1\,] \leqq [\,x_2\,] \;\longleftarrow$ 数直線でも描いて確認せよ！

しかし、この「 **逆はいえない** 」から注意のこと！

たとえば、$x_1=2.5,\ x_2=2.1$ などのときは $[\,x_1\,]=[\,x_2\,]=2$ で $[\,x_1\,] \leqq [\,x_2\,]$ は成り立つが $x_1 > x_2$ であり、逆の成り立たない例があることがわかる．

5° $\boldsymbol{[\,x_1\,]+[\,x_2\,] \leqq [\,x_1+x_2\,] \leqq [\,x_1\,]+[\,x_2\,]+1}$

上記「 **3°** 」より

$[\,x_1\,] \leqq x_1 < [\,x_1\,]+1, \qquad [\,x_2\,] \leqq x_2 < [\,x_2\,]+1 \cdots\cdots\cdots\cdots\cdots\cdots (*)$

$(*)$ のヘンペンを加えて

$[\,x_1\,]+[\,x_2\,] \leqq x_1+x_2 < [\,x_1\,]+[\,x_2\,]+2$

ここで、$[\,x_1\,]+[\,x_2\,]=n$ とおくと、これは $n \leqq x_1+x_2 < n+2$ だから、次のように場合を分けて考える．すなわち

(i) $n \leqq x_1+x_2 < n+1$ のとき

$[\,x_1+x_2\,]=n=[\,x_1\,]+[\,x_2\,]$

(ii) $n+1 \leqq x_1+x_2 < n+2$ のとき

$[\,x_1+x_2\,]=n+1=[\,x_1\,]+[\,x_2\,]+1$

したがって、$[\,x_1+x_2\,]$ は $[\,x_1\,]+[\,x_2\,]$ か、$[\,x_1\,]+[\,x_2\,]+1$ のいずれかであるから

$[\,x_1\,]+[\,x_2\,] \leqq [\,x_1+x_2\,] \leqq [\,x_1\,]+[\,x_2\,]+1$

なお、これは n 個の場合についても拡張できて

$$\begin{aligned}[\,x_1\,]+[\,x_2\,]+\cdots+[\,x_n\,] &\leqq [\,x_1+x_2+\cdots+x_n\,]\\ &\leqq [\,x_1\,]+[\,x_2\,]+\cdots+[\,x_n\,]+(n-1)\end{aligned}$$

さらに、$x_1=x_2=\cdots=x_n$ とおくと

$n[\,x\,]=[\,nx\,] \leqq n[\,x\,]+(n-1)$

も成り立つ．

5° $\boldsymbol{\left[\,\frac{a}{b}\,\right] \leqq \frac{a}{b} \leqq \left[\,\frac{a}{b}\,\right]+\left(1-\frac{1}{b}\right)}$、 **ただし $\boldsymbol{a}$ を整数、$\boldsymbol{b}$ を正整数とする．**

上記「 **3°** 」より

$\left[\,\frac{a}{b}\,\right] \leqq \frac{a}{b} < \left[\,\frac{a}{b}\,\right]+1 \qquad \therefore\;\; a < \left[\,\frac{a}{b}\,\right]b+b$

この両辺は整数で $b>0$ であるから

$a \leqq \left[\,\frac{a}{b}\,\right]b+b-1 \qquad \therefore\;\; \frac{a}{b} \leqq \left[\,\frac{a}{b}\,\right]+\left(1-\frac{1}{b}\right)$

となる．

第2章　応用編

ここでは**方程式や不等式の整数解**を求める方法について考えることにする．本来、整数問題の流れのなかで決着をつけてしまう方が確かにスッキリはする．

しかし、整数の性質を方程式や不等式の約束の中で扱うという 1 つ余計な配慮が絡みこむことと、書いているうちにもっと他の性質 (たとえばイデアルの概念) なども入り込んで内容が膨らんでしまったことによると考えてもらえばよい．

さりとて、あっさりと切り捨ててしまうのも心苦しい．まあ、知っておいてもソンはしないだろうという程度の親心である．

たとえば x, y についての方程式

$$3x + 5y = 45 \text{ (後述)}$$

を満たす整数解 x, y の値を求めるには、もし何も知らなければ

$$5y = 45 - 3x \qquad \therefore \quad y = 9 - \frac{3x}{5} \longleftarrow \ y \text{ が整数だから } x \text{ は } 5 \text{ の倍数！}$$

$$\therefore \quad x = 0,\ \pm 5,\ \pm 10,\ \pm 15,\ \cdots\cdots\cdots\cdots$$

を求めて、さらに代入して整数 y を求めることになるであろう．もちろんこれでよい．

これでよいのだが、われわれとしては、この手のものは一括して把握しておきたい．そして、できればこの手の方程式の根底に潜む性質をつかむことができればもっとウレシイことがあるかも知れない．そういう思いに駆られてついつい書いてしまったということだ———少し難しいかもしれないが許されよ．しかし、実際の入試でも、そうとは言わず、何気に出題されたりしていることも書き添えておこう．

そういう意味で、この部分を切り離して、あえて**応用編**とした．チョッとやりすぎたキライはあるが、ガマンできないほどのことでもあるまい．せいぜい頑張ってみて下さい．

2.1　方程式の整数解、他

「 係数が整数である方程式 」を満たす「 未知数の整数値 」を求めることを、**不定方程式**を解くといい、その解を**整数解**というのだが、その整数解が問題になるのは、方程式の数よりも未知数の数が多い場合である.

私たちの扱う不定方程式は、大体 1 次か 2 次くらいまでのところであるが、1 次の場合はともかくとして、2 次以上になるとかなり難しくなるので、きわめて特殊な場合しか扱えない———最近の研究によると、不定方程式の整数解を求める一般的な方法はないということが証明されている.

したがって、基本的な姿勢としては、個々の方程式の特殊性をとらえて処理するしかない、と思ってよい. まあ、そういう世界であるということをあらかじめ覚悟して進むことにしよう.

2.1.1　1 次の不定方程式

2.1.1.1　$ax + by = c$

もちろん $a,\ b,\ c$ は整数である．そして、この方程式が整数解をもつかどうかは、$a,\ b$ の最大公約数を g としたとき、「 **c が g の倍数であるかどうか** 」で決まる．

たとえば、$x,\ y$ は整数とする**不定方程式**

$$4x + 6y = 25$$

などは解がない——$4 = 2^2,\ 6 = 2 \cdot 3$ で、これらの「 G.C.M. 」は 2 だが、右辺の 25 は 2 の倍数ではないからである．

その**根拠**は

「 **$ax + by$ 形の整数全体の集合が、$a,\ b$ の最大公約数 g の倍数の集合に等しい** 」

という**事実**によるわけだが、ここでは、こういうことも含めてわかってもらいたい わけである．つまり

(i) まず、**整数解の存在**を確認する——トウアンには書かなくてよかろう．

(ii) 次に、それを**求める**にはどうすればよいか．

ということである——以下、詳しく解説する．

＜メモ＞

■ $\boldsymbol{ax+by=c}$ の解法について

まずは実例でやってみないことにはピンとこないだろう．カタチはスッキリしていて好感が持てそうだが、ドッコイそうはいかない———実は相当な**難物**なのである．

＜ 例 ＞

$6x+10y=90$ の整数解を求めよ．

(解) **ナイショの話**だが、$6=2\cdot 3,\ 10=2\cdot 5$ だから、これらの「 G.C.M. 」は 2 で、右辺の 90 はこの倍数だから**解は存在する**———安心して進めばよい．

そこで、まず両辺の係数は約せるだけ約して簡単にしておく．そうすると

$$\boldsymbol{3x+5y=45}\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\text{①}$$

となるから、これを満たすような x, y の整数値の組を、「 とりあえず 1 組 」見つける．

たとえば、$\boldsymbol{x=5,\ y=6}$ が ① を満たす．これが見つかれば ① にそのまま入れて

$$\boldsymbol{3\cdot 5+5\cdot 6=45}\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\text{②}$$

を作る———①から② を引いて定数 45 を消去するのだ．

ゆえに、 ① − ② より

$$3(x-5)+5(y-6)=0 \quad \therefore\ \ 3(x-5)=5(6-y)\ \cdots\cdots\cdots\cdots\cdots\text{③}$$

ここで、3 と 5 は**互いに素**であるから $x-5$ は 5 の倍数であるから k を整数として

$$x-5=5k \quad \therefore\ \ x=5k+5$$

$x-5=5k$ を ③ に入れると

$$3\cdot(5k)=5(6-y) \quad \therefore\ \ y=6-3k$$

以上から

$$x=5k+5,\ \ y=6-3k\ \ (k\text{ は任意の整数})$$

となる．これを**一般解**というのだが、しかし問題に、たとえば「 $x,\ y$ の正の整数解を求めよ 」などの要求があれば k に制限がつく．

$$x=5k+5>0,\ \ y=6-3k>0 \quad \therefore\ \ -1<k<2 \quad \therefore\ \ k=0,\ 1$$

ゆえに求める $x,\ y$ の組は 2 組あって

$$(x,\ y)=(10,\ 3),\ \ (5,\ 6)\ \longleftarrow\ \text{トケタ！}$$

★$_1$ 解法の流れを整理しておく

ここまでで、一体、何をやったのか．この先、ハナシが込み入ってくるので、ここで一旦まとめておく．上記をなぞって**一般の形**で整理しておくとよい．

そこで、与えられた方程式だが

$$\boldsymbol{ax+by=c}\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(*)$$

これは約せるだけ約した形のものとする．

まず、何でもよいから $(*)$ を満たす解を 1 組見つける———見つけ方はあとで詳しく述べる．そして、見つけた解を $(x_0,\ y_0)$ とすると、これは $(*)$ を満たす．すなわち

$$\boldsymbol{ax_0+by_0=c}\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(**)$$

$(*)-(**)$ を計算すると

$$a(x-x_0)=b(y_0-y)$$

ここで、$a,\ b$ に 1 以外の約数があれば、それで約してなるべく簡単な形にしておく．

$$\boldsymbol{a'(x-x_0)=b'(y_0-y)}$$

そうすると、a', b' は**互いに素**だから

$$\boldsymbol{x - x_0 = b'k} \quad \therefore \quad x = x_0 + b'k$$

したがって、これを入れると b' が約されて

$$y_0 - y' = a'k \quad \therefore \quad y = y_0 - a'k$$

と x, y の組が求まり

$$x = x_0 + b'k, \quad y = y_0 - a'k$$

これが**一般解**である．さらに、これに加えて、たとえば $x > 0$, $y > 0$ など条件がつけば

$$x_0 + b'k > 0, \quad y_0 - a'k > 0$$

などから k に制限がかかり、それを満たす整数 k の値から整数解 x, y が求まる．

まあ、こう振り返ってみて、ポイントは最初に 1 組の解 x_0, y_0 を見つけること であろう．いくつかやってみるとよい．

★$_2$ 「 1 組の解 」を見つける方法

上記では ① の係数が簡単で、「 **とりあえず必要な 1 組の解 $(x,\ y) = (5, 6)$** 」を簡単に見つけることができた———しかし、係数が少し大きくなるとそう簡単にはいかない．

そういうときのために、以下に述べる 2 つの方法を知っていると重宝である．

(i) **腕力で求める———「 係数を小さくしていく 」方法**

それには、まず、「 ① の x, y の係数は 3, 5 で**小さい方が 3** 」だから、3 で 5 を割る計算を利用する．すなわち、① から

$$3x = 45 - 5y \quad \therefore \quad x = \frac{45 - 5y}{3}$$

この右辺の分子 $45 - 5y$ を、3 で割れるだけ割って変形すると

$$x = 15 - \frac{3y + 2y}{3} \quad \longleftarrow \quad \boldsymbol{5y = 3y + 2y}$$
$$= 15 - y - \frac{2y}{3}$$

となり、x, y が整数だから $\dfrac{2y}{3}$ も整数で、したがって y は 3 の倍数である．

ここで、$y = 3$ としてもよいし、あるいは -3 としてもよい———符号にこだわらないのは、どのみち、「 あとで k の値で調整される 」からである．ともかく 3 の倍数を 1 つとり、それに対応する x の値を求めると、ともあれ ① を満たす整数解の 1 組を見つけることができる．

念のため、係数をもう少し大きくしてやってみる———ちょっと**工夫**が要ることがわかればよい．

$$\boldsymbol{21x + 8y = 123}$$

のようなときはどうするか．この例では **8 の方が小さい**ので

$$8y = 123 - 21x \quad \therefore \quad y = \frac{123 - 21x}{8}$$

そこで、$123 - 21x$ の変形を工夫する．

$$y = \frac{8 \cdot 15 + 3 - (2 \cdot 8 + 5)x}{8} \quad \longleftarrow \quad 8 \times 15 = 120, \quad (8x) \times 2 = 16x$$
$$= 15 - 2x + \frac{3 - 5x}{8}$$

x, y は整数だから、$3 - 5x$ は 8 の倍数で、そのような x の整数値の 1 つとして $x = -1$ が得られ、したがってこの場合、$y = 144$ となる．

しかし、それでも $3 - 5x$ が 8 の倍数になるような x が簡単に見つからないときは、「この方法 」を**繰り返し用いて**係数を小さくしていく、すなわち

$$3 - 5x = 8z \quad \longleftarrow \quad \boldsymbol{3 - 5x} \text{ を } \boldsymbol{8} \text{ の倍数とおいてしまえ！}$$
$$\therefore \quad 5x + 8z = 3$$
$$\therefore \quad x = \frac{3 - 8z}{5} = -z + \frac{3(1 - z)}{5}$$

$x,\ z$ が整数だから、$1-z$ が 5 の倍数で

$$z=-4 \quad \therefore\ x=7 \quad \therefore\ y=-3 \quad \longrightarrow\ (x,\ y)=(7,\ -3)$$

という 1 組の整数解が見つけることができる．そして、このような計算操作の基本原理は、実は**ユークリッドの互除法**である．

(ii) **実は、「 究極の方法 」がある**

それにしても、「 もっと簡単に 」、というより、「 いつでも確実に 」その 1 組の解 $(x_0,\ y_0)$ を見つける方法はないか．実は「 **究極の方法** 」がある．それは、先に $(*)$ で示した不定方程式

$$ax+by=c \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

で、**$a,\ b$ が互いに素**であるときは、この右辺の c を単純に 1 に置き換えた不定方程式 を作ると

$$\boldsymbol{ax+by=1}$$

だが、これを満たす整数 $x,\ y$ の組が必ずある ことがわかっている———**ここだ！**

本文でとりあげた例の

$$21x+8y=123$$

でいうと、21 と 8 は互いに素であるから、先に

$$21x'+8y'=1$$

となるような $(x',\ y')$ が 1 組求まる———123 と 1 とでは 1 のほうが**ダンゼン**見つけ易い．

たとえば、$x'=-3,\ y'=8$ がすぐに見つかる．そうすると、数値は少し大きくなるが

$$21\cdot(-3)+8\cdot 8=1 \ \longleftarrow\ \textbf{この両辺に 123 をカケル！}$$

$$21\cdot\underbrace{(-3\cdot 123)}_{x}+8\cdot\underbrace{(8\cdot 123)}_{y}=123$$

となり

$$x=-3\cdot 123=-369, \qquad y=8\cdot 123=984$$

で、これが $21x+8y=123$ の 1 組の解であることがわかる．

と、まあ、こんな具合だが、ハナシがうますぎる———不定方程式 $\boldsymbol{ax+by=c}$ に対して、どうしてこんなに都合よく $\boldsymbol{ax+by=1}$ が用意されるのか．それは、冒頭で

「 **$ax+by$ の形の整数全体の集合が $a,\ b$ の最大公約数 g の倍数の集合に等しい** 」

と大見得を切ったが、そのハナシはこの「 **定理** 」に集約されるのである．

上記の「 $21x+8y$ 」で 21 と 8 とは互いに素であるから、その最大公約数は $g=1$ で、その倍数の集合になるはずだから、最も簡単な「 1 」はその中にあるはずである．そこで、まず

$$21x'+8y'=1$$

となるような $(x',\ y')$ を 1 組求めておいて、あとは上記の展開の通りである．

この問題に関してだけなら「 結果、オーライ！ 」でよいが、しかし、その「 **ワケをわかりたい** 」となると、どうしても上記の定理を乗り越えなくてはならない．

つまり、それは**整数の性質**についての「 1 ランク上の議論 」にならざるを得ない．そういうわけで、このハナシは一旦、仕切りなおしてとりかかることにする．

＜ end. ＞

■ 「 究極の方法 」のルーツを訪ねて

先に述べたように、a, b が互いに素な整数であるとき、**不定方程式**

$$\boldsymbol{ax + by = 1}$$

の解が「 **必ず存在する** 」ことが説明されれば、**問題の核心**が解決することになる.

以下、その解説をするのだが、どうもこのハナシだけでオシマイにするのはあまり生産的でない、というより、せっかくの素材がもったいない.

そこで、ちょっと敷居は高いが、ここでは「 **構造的代数** 」といわれる現代数学の考え方、特にその中の**イデアル**という考え方を借りて解説することにした.

もちろん、これは高校の教科書には出てこないので、多少の違和感があるかも知れないが、「 その方が**ストレート**、かつ**明快**にナットクしてもらえるであろう 」という筆者の独断と偏見によるものと思ってもらってよい. しかし、「そうは言っても ……」という向きもあろうかと思われるので、できる限り従来の論証の方法を踏まえた説明も入れた.

さて、その解説は

＜1＞ イデアルとは何か
＜2＞ 集合 $\{z \mid z = ax + by,\ x \in Z,\ y \in Z\}$ はイデアルなのだ
＜3＞「 イデアル 」の整数論への応用

の手順で進めるが、われわれの目指す「 **究極の方法** 」のルーツは **＜3＞「 イデアル 」の整数論への応用**の「 **定理 3** 」であることをあらかじめ予告しておく.

このゴールに向かってイッキに駆け抜けてもらいたい. なお**＜3＞**では、この定理のあとに、「 すでに解説した約数、倍数に関する定理のいくつか 」をイデアルの立場から説明した.

このようなカタチでの解説では、多少雑駁な説明にならざるを得ないが、イデアルの考え方の**威力**、その**雰囲気**は感じてもらえるかと思う.

＜1＞ イデアルとは何か

ここで、整数の基本的性質の 1 つである「 **イデアル** 」という数学的概念を用意しておかなければならない———このハナシはここから出発する.

イデアルの定義

Z の部分集合 S が、次の条件を満たすとき、S は Z の**イデアル**という. すなわち

1° S は 0 でない整数を含む.

2° $a \in S,\ \ b \in S$ ならば $a - b \in S$ である.

(解説) この「 2° 」は、S が**減法**について**閉じている**ことを示しているが、このイデアルの定義を、**加法**を用いて、次のように定義してもよい. すなわち

1° S は 0 でない整数を含む.

2° $a \in S,\ \ b \in S$ ならば $a + b \in S$ である.

3° $a \in S,$ ならば $-a \in S$ である.

を満たす Z の部分集合 S を Z のイデアルという、と言い換えてもよい. 実はこれらは同じことを表しているのである———次に述べる定理 1 で明らかにする.

また、「 イデアル 」の考え方の応用は何も整数の集合に限ったハナシではなく手近の例では、整数とよく似た扱いのできる実数係数の一元 (1 文字 x) の多項式などでも構成される.

しかし、ここではハナシをシンプルにしておきたいので深入りはしない———そういう展開もあり得ることが予感できれば十分ある.

＜ end. ＞

さて、この定義から出発して次の定理が導かれる．すなわち

定理 1

S が Z のイデアルであるとき、次の (1)〜(3) が成り立つ．すなわち

(1) $\boldsymbol{a \in S,\ b \in S \implies a+b \in S}$

(2) $\boldsymbol{a \in S \implies na \in S}$

(3) S は、その要素の中に最小の正整数 d を持ち、**S は d の倍数全体の集合と一致する．**

（証明） 実は、これらがあとで効いてくる———順に証明しておく．

(1) 先に述べた「 **定義 1°** 」で $b=a$ とおくと

$$a-b=a-a=0 \in S$$

つまり、0 が S の要素である———これを使う．そこで、再び「 **定義 1°** 」で $a=0$ とおくと

$$0-b=-b \in S$$

さらに「 **定義 1°** 」が使えて $a \in S,\ -b \in S$ だから

$$a-(-b)=a+b \in S \longleftarrow \text{デキタ！}$$

(2) (1) の結果を使う———基本的には**数学的帰納法**である．

(i) $n=1$ のときは、明らかに成り立つ．

(ii) $n=k$ のとき成り立つと仮定すると、$ka \in S$ であるから、$a \in S$ とあわせて

$$ka+a=(k+1)a \in S$$

すなわち、任意の自然数 n に対して $na \in S$ である．

また、$0 \in S,\ na \in S$ であるから、任意の整数 n に対して

$$0-na=-na \in S$$

ゆえに、すべての整数 n に対して $na \in S$ である．

(3) まず、集合 S に正整数が存在することを確認しなければならない．

「 **定義 1°** 」より S は「 0 でない整数を含む 」から、それを a とする．そうすると、$-a \in S$ だから、a と $-a$ の一方は正整数で、集合 S は必ず正整数を含む———トウゼンだ．

だから、正整数の集合には最小値が存在するのでそれを d とすれば

$$a=dq+r \quad (0 \leqq r < d) \qquad \therefore\ r=a-dq$$

となる整数 $q,\ r$ がただ 1 組だけ存在する．

ここで、「 $d \in S,\ q$ は整数 」であるから、「 **定理 (2)** 」より $dq \in S$ である．したがって、「 定義 2° 」より

$$a-dq \in S \qquad \therefore\ r \in S$$

今、$r \neq 0$ とすると r は d より小さい正整数だから、「 d が最小 」という条件に反するし、$r=0$ でなければならない．すなわち、S の任意の要素 a は d の倍数である．また、「 **定理 (2)** 」より、S は d の倍数全体の集合である．

★ $ax+by$ への準備

(1) と (2) の結果を併せて使えば、その要素が $ax+by$ のカタチで表される集合が**イデアル**であることはタダチにわかる．

さらに、これと併せて (3) は次の「 **定理 2** 」への準備である．

＜ end. ＞

＜2＞ 集合 $\{z \mid z = ax + by,\ x \in Z,\ y \in Z\}$ はイデアルなのだ

$x,\ y$ を変数とするとき、1 次の同次式 $\boldsymbol{ax + by}$ を $x,\ y$ の **1 次結合**というのだが、$a,\ b$ が与えられた整数で、$x,\ y$ が任意の整数であるとき、「 $ax + by$ の形の整数全体の集合 M 」はイデアルである――やっと**論点**にたどりついた．

何だか、最初の目的が何であったのかわからなくなるくらい、遠くに来てしまったような気がする．改めて、それが何であったかを確認しておきたい．それは

「 **$ax + by$ の形の整数全体の集合が $a,\ b$ の最大公約数 g の倍数の集合に等しい** 」

というその**理由**が知りたかった――以下、「 **定理** 」の体裁にして論点を明確にする．

定理 2

$a,\ b$ を与えられた 0 でない整数として、集合

$$M = \{z \mid z = ax + by,\ \ x \in Z,\ y \in Z\}$$

について、次の定理が成り立つ．

(1) $a \in M,\ b \in M$ である．

(2) M はイデアルである．

(3) M は、$a,\ b$ の最大公約数の倍数の集合である．

(4) N がイデアルであるとき、$a \in N,\ b \in N$ ならば $M \subseteqq N$ である．

(証明) この (3) が証明できれば、ここまでの目的は達成される――(1) と (2) はその準備である．また、(4) はこの先の展開をにらんだ定理であると思ってもらいたい．

(1) $x,\ y$ は任意の整数としてよいから

$$x = 1,\ y = 0 \ \longrightarrow\ ax + by = a \cdot 1 + b \cdot 0 = a \in M$$
$$x = 0,\ y = 1 \ \longrightarrow\ ax + by = a \cdot 0 + b \cdot 1 = b \in M$$

(2) イデアルの条件である「 **定義 1°** 」については (1) から

$$a\ (\neq 0) \in M,\ \ b\ (\neq 0) \in M \ \longleftarrow\ \text{どちらかを示せばよい！}$$

「 **定義 2°** 」については、M の任意の 2 つの要素 $p,\ q$ を

$$p = ax_1 + by_2,\quad q = ax_2 + by_2 \qquad (\ x_1,\ y_1,\ x_2,\ y_2 \text{は整数！})$$

とすると、$p - q$ が M の要素であることをいえばよいから

$$p - q = a\underbrace{(x_1 - x_2)}_{\text{整数}} + b\underbrace{(y_1 - y_2)}_{\text{整数}} \ \in M \ \longleftarrow\ \text{いえた！}$$

ゆえに、集合 M はイデアルである．

(3) これはかなり難しい――論証の仕方に慣れるよい機会である．

イデアル M には**最小の正整数 d** が存在し、M がその d の倍数の集合であることは前掲の「 **定理 1** 」で述べたから、これは問題なしとする．

そうすると a も b も d の公約数でなければならない．そこで

$$a = l_1 d,\ \ b = l_2 d \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

とおくと、「 **$l_1,\ l_2$ が互いに素** 」であれば d は $a,\ b$ の**最大公約数**ということになる．

したがって、それを言うには $l_1,\ l_2$ が 1 以外に正の公約数をもたない (互いに素) ことを証明すればよい――これがなかなか難しい．

さて、d は M の要素であるから $m_0,\ n_0$ を整数として

$$d = am_0 + bn_0$$

と表される．これに $(*)$ を入れると

$$d = (l_1 d)m_0 + (l_2 d)n_0 = d(l_1 m_0 + l_2 n_0)$$

$d > 0$ だから両辺を d で約すと

$$l_1 m_0 + l_2 n_0 = 1 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (**)$$

ここで、$l_1,\ l_2$ が互いに素でないとすると、1 以外に正の公約数 g $(\geqq 2)$ をもつはずだから

$$l_1 = gm_0',\quad l_2 = gn_0' \qquad (m_0',\ n_0' \text{は整数})$$

だから、これを $(**)$ に入れて

$$g\underbrace{(m_0 m_0' + n_0 n_0')}_{\text{整数}} = 1$$

ここで、$m_0 m_0' + n_0 n_0'$ は整数だから、2 以上の整数 g が 1 の約数となって不合理である．つまり $l_1,\ l_2$ は互いに素で、d は $a,\ b$ の最大公約数である．

(4) N は**イデアル**だから「 **定理 1(3)** 」より、「 N はその**最小の正整数 d'** の倍数の集合 」である．このとき

$$a \in N,\ b \in N \ \longrightarrow\ a = d'a',\quad b = d'b'$$

このとき、集合 M の任意の要素である z は

$$\begin{aligned} z &= ax + by \\ &= (d'a')x + (d'b')y = d\,(a'x + b'y) \ \longleftarrow\ d'\text{の倍数！} \\ &\quad \therefore\ \ z \in N \end{aligned}$$

すなわち、$M \subseteqq N$ であることが示された．

★ **ハナシの拡張**

ここで証明は終えるが、このハナシはさらに拡張できて、$a_1,\ a_2\ ,\cdots\cdots,\ a_n$ を与えられた整数とし、$x_1,\ x_2\ ,\cdots\cdots,\ x_n$ を任意の整数とするとき

$$a_1 x_1 + a_2 x_2 + \cdots\cdots + a_n x_n$$

の形の整数全体の集合 M はイデアルであって、$a_1,\ a_2\ ,\cdots\cdots,\ a_n$ の最大公約数を d とすると、M は d の倍数の集合と一致する——この証明も $ax + by$ の場合とほとんど同様である．

したがって、一般の**不定方程式**は

$$\boldsymbol{a_1 x_1 + a_2 x_2 + \cdots\cdots + a_n x_n = b}$$

だが、これが解をもつかどうかは、「 右辺の**定数 b** が上記の**最大公約数 d** の倍数であるかどうか 」で決まる——これは知っていなければならない．

特に $\boldsymbol{ax + by = c}$ の場合は、その 1 組の解を $(x_0\ y_0)$ とすると、その**一般解**は

$$x = x_0 + \left(\frac{b}{d}\right)k, \qquad y = y_0 - \left(\frac{a}{d}\right)k \qquad (k = 0, \pm 1, \pm 2,\ \cdots\cdots)$$

となる．

＜ end. ＞

＜例＞

$m,\ n,\ p,\ q$ が整数全体をとってかわるとき、$12m+8n$ の形の整数全体の集合を M とし、$20p+16q$ の形の整数全体の集合を N とする．このとき $M=N$ であることを示せ．

(解) イデアルについての知識がなければ、$\boldsymbol{M=N}$ を示す基本的な方法は

$$\boldsymbol{M \subseteqq N,\ かつ\ M \supseteqq N}$$

だから、これを示す方向に考え方を進めていくだろう———やっておく．

(i) $\boldsymbol{M \subseteqq N}$ **を示す．**

これには、M の任意の要素を x とすると

$$x=12m+8n$$

だから、これが $20p+16q$ の形に書き換えられることを示せばよい．つまり

$$\begin{aligned} x &= 12m+8n \\ &= 20\underbrace{(3m+2n)}_{p}+16\underbrace{(-3m-2n)}_{q}=20p+16q \in N \end{aligned}$$

したがって、$M \subseteqq N$ である．

(ii) $\boldsymbol{M \supseteqq N}$ **を示す．**

同様にして、N の任意の要素を y とすると

$$\begin{aligned} y &= 20p+16q \\ &= 12\underbrace{(5p+4q)}_{m}+8\underbrace{(-5p-4q)}_{n}=12m+8n \in M \end{aligned}$$

となり、これらの考察から $M=N$ が示された、となるが、なかなかヤッカイである．

しかし、イデアルについての知識があれば

12 と 8 の最大公約数は 4 $\longrightarrow$ $\boldsymbol{M}$ は 4 の倍数全体の集合

20 と 16 の最大公約数は 4 $\longrightarrow$ $\boldsymbol{N}$ は 4 の倍数全体の集合

であることがすぐにわかるので、そのような方向にその証明をもっていけばよい．

すなわち、M の任意の要素 x は

$$x=12m+8n=4(3m+2n) \longleftarrow \text{4 の倍数！}$$

しかし、これだけでは「 4 の倍数全体 」の集合とはいえない．つまり、この「 逆に、4 の倍数であるものはすべて M の要素になっている 」ことを示さなければならない．

そこで、任意の 4 の倍数を $4k$ とおくと

$$4k=12k+8(-k)$$

と変形されることに注目して、$k=m,\quad -k=n$ とおくと

$$4k=12m+8n \in M$$

となる．したがって、M は 4 の倍数全体の集合であることがわかる．

同様にして N も 4 の倍数全体の集合であることをいえば $M=N$ が示されたことになる．

＜ end. ＞

＜3＞「 イデアル 」の整数論への応用

まず、定理を 1 つあげておく．これは冒頭の＜例＞で、1 組の解 $(x_0,\ y_0)$ を求めるとき、「 **究極の方法がある** 」と言って使ったその方法の根拠である——やっと出てきた．

実はそれだけではなく、結構その応用範囲の広い定理である．そのすべてをここで解説する．

定理 3

$a,\ b$ が互いに素な整数であるときは

$$ax + by = 1$$

を満たす整数 $x,\ y$ が存在する．

（証明） イデアルの知識があれば、$a,\ b$ が互いに素ということは、その最大公約数が 1 ということだから、集合

$$M = \{z|\ z = ax + by,\ x \in Z,\ y \in Z\}$$

は 1 の倍数の集合であり、M がどんな整数をもその要素としてもつから $ax + by = 1$ を満たす整数値があるのは「 **当たり前** 」のことである——**証明はこれで終わり！**

しかし、イデアルの定理を用いないでやることも知っていなければならない．せっかくの機会だからやっておく．

まず、M に含まれる**最小の正整数**を $\boldsymbol{d = at + bu}$ **($t,\ u$ は整数)** とおく．そうすると

$$a = dq + r,\quad 0 \leqq r < d \quad \longleftarrow \text{ 整除の定理！}$$

となる整数 $q,\ r$ が 1 組存在する．これから

$$\begin{aligned} r &= a - dq \\ &= a - (at + bu)q = a\underbrace{(1 - qt)}_{\text{整数}} + b\underbrace{(-qu)}_{\text{整数}} \in M \end{aligned}$$

ここで、$r \neq 0$ とすると M は d より小さい整数 r を含むことになり条件に反する．

ゆえに $r = 0$ で

$$a = dq \ \longrightarrow\ d \text{ は } a \text{ の約数！}$$

同様にして、d は b の約数であることも証明できるから、d は $a,\ b$ の正の約数である．

ところが、$a,\ b$ は互いに素であるから $d = 1$ で

$$\boldsymbol{d = at + bu = 1}$$

すなわち、$ax + by = 1$ を満たす整数の組 $(t,\ u)$ が存在する．

★ **この定理は「 逆 」も成り立つ．**

すなわち

「 **$a,\ b,\ x,\ y$ が整数で**

$$\boldsymbol{ax + by = 1}$$

が成り立つときは、$a,\ b$ は**互いに素**である 」ともいえて、なかなか重宝だ——知っておくべきことがらである．

以下、これらのことをもとにして、前に述べた整数に関するいくつかの定理をながめてみよう——**イデアル**を知る以前とちがった感触が得られれば筆者としては大満足である．

＜ end. ＞

以下、「 **1.2.1 約数・倍数** 」で述べた定理だが、**イデアル**の立場ではどう扱うか．まあ、蛇足といえばそれまでだが、**検証**しておくこともよいことではある———堪能してもらいたい．

定理 4

(1) $a,\ b$ が互いに素で、ac が b で割り切れるなら、c は b の倍数である．

(2) 整数 $a,\ b$ の最大公約数を d、最小公倍数を l とし、$a = a'd,\ b = b'd$ とすれば

(i) $a',\ b'$ は互いに素　(ii) $l = a'b'd$　(iii) $ab = ld$

である．

(証明) (1) これはほとんど「 当たり前 」である．

それは、整数の「 素因数分解の一意性 」から言っても明らかであるが、厳密に証明しようとすると前掲の「 **定理 (3)** 」を使うことになる．

整数 $a,\ b$ が互いに素であるから

$$\boldsymbol{ax + by = 1}$$

を満たす整数 $x,\ y$ の組が存在する．そこで両辺に c をカケルと

$$cax + cby = c$$

条件から ac が b で割り切れるから、$ac = bk$ (k は整数) とおくと

$$(bk)x + cby = c \qquad \therefore\ \ b(kx + cy) = c$$

ここで、$kx + cy$ は整数だから c は b の倍数である．

(2) まず (i) だが、$a,\ b$ の最大公約数 d は、「 **定理 (3)** 」の証明で用いた M の要素であるから

$$\boldsymbol{d = ax + by} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

を満たす整数 $x,\ y$ がある．これに $a = a'd,\ \ b = b'd$ を入れて

$$d = (a'd)x + (b'd)y \qquad \therefore\ \ \boldsymbol{a'x + b'y = 1}$$

したがって、「 **定理 (3)** 」の逆より $\boldsymbol{a',\ b'}$ **は互いに素**である ことがわかる．

(ii) については

$$\boldsymbol{a'b'd = ab' = a'b}$$

であるから、$a'b'd$ は $a,\ b$ の公倍数 である．

そこで、$a,\ b$ の任意の公倍数を n として $n = au = bv$ ($u,\ v$ は整数) とおくと $(*)$ から

$$\begin{aligned} nd &= n(ax + by) = nax + nby \\ &= (bv)ax + (au)by = ab(vx + uy) = a'b'd^2(vx + uy) \\ &\qquad \therefore\ \ n = a'b'd(vx + uy) \end{aligned}$$

よって、n は $a'b'd$ の倍数であり、このような正整数 n の最小のものは $a'b'd$ であるから、$a,\ b$ の最小公倍数 l は $a'b'd$ に等しい．

(iii) これは簡単にいく．

$$\begin{aligned} ab &= (a\ d) \cdot (b'd) \\ &= (a'b'd) \cdot d = ld \end{aligned}$$

となる．

＜ end. ＞

定理 5

a を b で割った商を q、余りを r とするとき、$a,\ b$ の最大公約数と $b,\ r$ の最大公約数は一致する.

（証明） これは、すでに述べた**ユークリッドの互除法**を支える基本原理である.
すなわち

$$\boldsymbol{a = bq + r,\quad 0 \leqq r < b} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

$\longleftarrow$ 整除の定理！

において、「 $\boldsymbol{a,\ b}$ **の最大公約数と** $\boldsymbol{b,\ r}$ **の最大公約数は一致する** 」ことを主張している.
さて、イデアルではこれをどう扱うか. その考え方を適用すると、2 つの集合

$$\boldsymbol{M = \{z|\ z = ax + by,\quad x \in Z,\ y \in Z\}} \longleftarrow \boldsymbol{a,\ b}\ \text{の最大公約数の倍数の集合！}$$

$$\boldsymbol{N = \ \{z|\ z = rx + by,\quad x \in X,\ y \in Z\}} \longleftarrow \boldsymbol{b,\ r}\ \text{の最大公約数の倍数の集合！}$$

が「 **一致する** 」ことをいえばよいハナシに置き換わる——それぞれが、a と b、b と r の**最大公約数の集合**だからこのように表される のだ——これは有難い.
そこで、M の任意の要素を z_1 とすると

$$z_1 = ax_1 + by_1\ (x_1,\ y_1\text{は整数})$$

だから、これに $(*)$ を入れて

$$z_1 = (bq + r)x_1 + by_1 = r\underbrace{x_1}_{\text{整数}} + b\underbrace{(qx_1 + y_1)}_{\text{整数}} \in N$$

であるから $M \subseteqq N$ であることがわかる.
同様にして $M \supseteqq N$ もいえるので、$M = N$ である.

＜ end. ＞

2.1.1.2　$ax + by + cz = d$

この形の不定方程式も、考え方の基本原理は 2 文字の場合と同じだが、3 文字になると結構ヤッカイである——初回はトバシて読んでもよい.

この場合も、2 文字のときと同様に $a,\ b,\ c$ の最大公約数を g とすると、d が g の倍数であれば整数解があり、そうでなければ整数解はない.

以下、実例で説明する.

＜メモ＞

■ $\boldsymbol{ax+by+cz=d}$ を解く

基本原理は同じでも、3 変数となると 2 変数の場合と扱い方は全くちがう．たとえば、3 変数の不定方程式

$$ax+by+cz=d$$

に対して、1 組の解 $(x_0,\ y_0,\ z_0)$ が求まったとしても、そして、これらが上記を満たすことから

$$ax_0+by_0+cz_0=d$$

が成り立ったとしても、そしてヘンペン引いて

$$a(x-x_0)+b(y-y_0)+c(z-z_0)=0$$

さて、この先どうするか――これで**行き止まり**なのである．

それでも無理やりやろうとすれば、基本的には 2 変数の扱いを組み合わせて 3 変数を処理するしかない．以下、例題で具体的に説明する．

＜例＞

$4x+6y+17z=5$ の整数解を求めよ．

(解) 与えられた方程式を

$$2\underbrace{(2x+3y)}_{u\ とおく}+17z=5 \longrightarrow \begin{cases} 2x+3y=u \cdots\cdots\cdots\cdots\cdots\cdots ① \\ 2u+17z=5 \cdots\cdots\cdots\cdots\cdots\cdots ② \end{cases}$$

とみて、まず ①と② を別々に解いて、あとでパラメーターを調整する．

(i) ① を解く――2 変数のときと全く同様だ．**2 と 3 が互いに素** であることを確認して

$$\boldsymbol{2x+3y=1} \longleftarrow \text{「イデアル」で定理として説明した！}$$

としてこの解を見つけるのだが、それは $x=-1,\ y=1$ としてすぐに求まるから

$$2\cdot(-1)+3\cdot 1=1$$

① の右辺に合わせて u 倍すると

$$2(-u)+3\cdot u=u \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ③$$

① − ③ より

$$2(x+u)+3(y-u)=0 \qquad \therefore\ \ \boldsymbol{2(x+u)=3(u-y)}$$

これより $x+u$ は 3 の倍数だから v を整数として

$$\begin{cases} x+u=3v \qquad \therefore\ \ x=-u+3v \\ u-y=2v \qquad \therefore\ \ y=u-2v \end{cases} \cdots\cdots\cdots\cdots\cdots\cdots (*)$$

(ii) ② を解く――同様に、**2 と 17 が互いに素** であることを確認して

$$\boldsymbol{2u+17z=1} \longleftarrow \text{「イデアル」で定理として説明した！}$$

としてこの解は $u=-8,\ z=1$ としてすぐに求まるから

$$2\cdot(-8)+17\cdot 1=1$$

② の右辺に合わせて 5 倍すると

$$2(-40)+17\cdot 5=5 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ④$$

② − ④ より

$$2(u+40)+17(z-5)=0 \qquad \therefore\ \ \boldsymbol{2(u+40)=17(5-z)}$$

これより $u+40$ は 17 の倍数だから w を整数として

$$\begin{cases} u+40=17w & \therefore\ \ u=17w-40 \\ 5-z=2w & \therefore\ \ z=5-2w \end{cases}$$

で、一応、$x,\ y,\ z$ の整数値は求まった．ここで、パラメーターは $u,\ v,\ w$ の 3 つに見えるが、上記を $(*)$ に代入すると、結局 u は消えて $v,\ w$ の 2 つになる．すなわち

$$\begin{cases} x=3v-17w+40 \\ y=-2v+17w-40 \\ z=5-2w \end{cases} \qquad \longleftarrow\ \ u,\ v \text{ は任意の整数！}$$

となるが、結局「 パラメーターの個数が、2 変数のときより 1 つ増えて 2 個になる 」ことに注目しておきたい．また、「 $x,\ y,\ z$ の正整数解を求めよ 」などの条件があれば

$$3v-17w+40>0,\ \ -2v+17w-40>0,\ 5-2w>0$$

を満たす $v,\ w$ の整数値を求めて $x,\ y,\ z$ を求めればよい．

★ 係数の小さい不定方程式に置き換える

他に方法がないわけではない．

$$4x+6y+17z=5$$

をみると、どうも係数が大きすぎる——これを小さくして扱う方法はないか．

まず、最も小さい x の係数 4 に注目して、y の係数 6 と z の係数 17 など、**係数の小型化**をはかる．これは、すでに**互除法**のところで解説したハナシの応用編である．そういう目で見ると

$$6=4\times1+2,\qquad 17=4\times4+1$$

だから、上記は

$$4x+(4\cdot1+2)y+(4\cdot4+1)z=5$$

$$\therefore\ \ 4\underbrace{(x+y+4z)}_{u\ \text{とおく}}+2y+z=5 \qquad \longrightarrow \begin{cases} x+y+4z=u \cdots\cdots\cdots\cdots(*) \\ 4u+2y+z=5\cdots\cdots\cdots\cdots(**) \end{cases}$$

ここで y の係数 2 に注目して $4=2\times2$ を用いて第 2 式で同じ変形をすると

$$2\cdot2u+2y+z=5 \qquad \therefore\ \ 2\underbrace{(2u+y)}_{v\ \text{とおく}}+z=5 \qquad \therefore\ \ 2v+z=5$$

$$\longrightarrow \begin{cases} 2u+y=v \\ 2v+z=5 \end{cases} \qquad \therefore\ \begin{cases} y=v-2u \\ z=5-2v \end{cases}$$

これらを $(*)$ に入れて

$$\begin{aligned} x&=u-y-4z \\ &=u-(v-2u)-4(5-2v)=3u+7v-20 \end{aligned}$$

これらをまとめると、結局

$$\begin{cases} x=3u+7v-20 \\ y=v-2u \\ z=5-2v \end{cases} \qquad \longleftarrow\ \ u,v \text{ は任意の整数！}$$

で、先に示した解答とはちがったカタチになるが、その内容は同じものである．

このやり方を振り返ってみると $(*)$ の「 x の係数が 1 となるようにおいた 」ところが決め手になっている．後半は $(**)$ の処理をしただけだが、$y,\ z$ の係数が 1 となるように調整したところがポイントである．

＜ end. ＞

2.1.2　2 次の不定方程式

2 次となると 1 次の場合ほど単純ではなく、その種類もぐっと多くなる．たとえば、古くから知られている**ピタゴラスの方程式**というのがある．

$$x^2 + y^2 = z^2 \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

の整数解を求める問題だが、この 1 組の解

$$x = 3,\quad y = 4,\quad z = 5$$

はよく知られている．そうすると

$$x = 3k,\quad y = 4k,\quad z = 5k \quad (k \text{ は任意の整数})$$

はすべて $(*)$ を満たすから、求める整数解は無数にあることになる．

この他にも

$$(x,\ y,\ z) = (\ 5,\ 12,\ 13\ ),\quad (\ 8,\ 15,\ 17\ )$$

など、いろいろな整数解があり、1 組だけ見つかったからといって、1 次のときのようにすぐに一般解が求まるものではない．さらに

$$\boldsymbol{x^n + y^n = z^n \quad (\ n \text{ は } 3 \text{ 以上の正整数}\ )}$$

となると、トタンに整数解がみつからなくなる．

そしてフェルマー (1608〜1665) は、「 $n \geqq 3$ ではこの方程式には整数解がない 」と言っている——これが有名な**フェルマーの問題**である．

フェルマーは彼の愛読書であったディオファントスの「 数論 」の欄外に、「 私は、これに対するすばらしい証明を知っているが、この余白がせますぎて書けない 」と書き込んでいる．その後、多くの人々の努力にもかかわらず、そして、どう見てもまちがいのない命題と言えそうであるにもかかわらず、さらには、この証明に賞金がかけられているにもかかわらず、最近までその証明はなされていなかった．

しかし、それも 1995 年、イギリスの数学者アンドリュー･ワイルズ (Andrew Wiles 1953 年 4 月 11 日〜) により証明され大きな話題になった——いろいろなエピソードもあっておもしろいから調べてみるとよい．

ともあれ、このように不定方程式には、一見やさしそうに見えていて、しかもこのような難問があるのである．したがって、これからとりあげる $x,\ y$ の 2 次の不定方程式も、ごく限られた特殊なものであると思ってよい．

2.1.2.1　$axy+bx+cy+d=0$

この不定方程式に限らず、考え方の基本は次の 2 つである．すなわち、未知数、またはそれを含む式の

(i) **約数、倍数に関する性質**に注目する．
(ii) **とり得る値の制限**を調べる．

ということである．

たとえば、$2x-1$ が 3 の倍数であって、$1<2x-1<10$ であることがわかったとしよう．そうすると $2x-1$ は奇数でもあるので

$$2x-1=3,\ 9 \quad \therefore\ \ x=2,\ 5$$

のように x の整数値が決まる．もちろん、いつも上記 (i) と (ii) の両方を調べなければならないというわけでもなく、他の条件との関係からそのどちらか一方だけで間に合うときもある．特にこの

$$axy+bx+cy+d=0 \quad (a,\ b,\ c,\ d \text{ は整数})$$

のカタチをしたものは

$$\underbrace{(px+q)}_{\text{整数}}\underbrace{(ry+s)}_{\text{整数}}=k$$

と変形するのがポイントで、これは「 $px+q,\ \ ry+s$ が整数 k の約数である 」というところから $x,\ y$ を求めていく典型的なタイプである．

以下、実例で解説する．

＜メモ＞

■ $\boldsymbol{axy+by+cz+d=0}$ 型 の不定方程式

＜例＞

$2xy+8x-y=16$ の整数解を求めよ．

(解) $x,\ y$ を含んだ部分を**積の形**に変形する．

$$\begin{aligned} 2xy+8x-y &= y(2x-1)+4(2x-1+1)\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(*) \\ &= (2x-1)(y+4)+4=16 \\ \therefore\quad (2x-1)(y+4) &= 12 \end{aligned}$$

x, y は正整数だから $2x-1>0,\ y+4>0$ 、しかも $2x-1$ は奇数で 12 の約数である．
これを表にして表すと

$2x-1$	1	3
$y+4$	12	4

$\therefore$

x	1	2
y	8	0

の 2 組が得られるが、第 2 組は $y>0$ に反するから除いて

$$x=1,\quad y=8$$

が求める正整数解である．

★ 割り落とす

しかし、筆者は $(*)$ の計算があまり得意でない．そういうときは、与えられた方程式が、たとえば、y について 1 次方程式であることに注目して y について解く——x について解いても同様である．

$$(2x-1)y+8x=16$$

$$\therefore\quad \boldsymbol{y=\frac{-8x+16}{2x-1}=-4+\frac{12}{2x-1}}$$

そうすると、y が正整数だから、$2x-1>0$ は奇数で 12 の約数でなくてはならない．
ゆえに

$$2x-1=1,\quad 3 \qquad \therefore\quad x=1,2$$

が得られて、あとは上記と同様の扱いとなる．

＜ end. ＞

2.1.2.2　判別式の利用

$x,\ y$ の 2 次方程式の一般形

$$ax^2 + hxy + by^2 + fx + gy + c = 0 \quad (a \neq 0)$$

についていうと、これを $\boldsymbol{x}$ **について整理**して

$$ax^2 + (hy + f)x + (by^2 + gy + c) = 0$$

$x,\ y$ が整数ならば、もちろんこれらは実数だから、「 x についての 2 次方程式 」とみて**判別式**を D とおくと

$$\begin{aligned} D &= (hy + f)^2 - 4a(by^2 + gy + c) \ \longleftarrow\ y \text{ について整理！} \\ &= py^2 + qy + r \end{aligned}$$

の形にまで変形する．あとは

(i) **実数条件** ： $D \geqq 0$ から $\boldsymbol{y}$ **の制限**を調べる．
(ii) $\boldsymbol{D =}$ **(整数)^2** ： x が整数であるためには D が整数の平方！

の 2 通りの考え方がある．

しかし、ここから整数 y が求まったとしても、これは**必要条件**で、実際には「 その中から x が整数値になるものを拾う 」ことになる．

＜メモ＞

■ 判別式の利用――扱い方は **2** つ

2 次の不定方程式で判別式を利用する場合、「 与えられた方程式のタイプ 」によって、次の **2** 通りの扱い方がある．

＜ 例 ＞

次の方程式を満たす $x,\ y$ の整数値を求めよ．

(1) $x^2 - xy + 3y^2 - 4x - 5y - 6 = 0$

(2) $2xy - 4x^2 + 12x - 5y = 11$

(解) (1) 与えられた方程式を x の 2 次方程式とみて、x について整理する――y の 2 次方程式とみて、y について扱ってもよい．

$$x^2 - (y+4)x + (3y^2 - 5y - 6) = 0 \cdots\cdots ①$$

これが整数解 x をもつ条件だが、整数はトウゼン実数だから、判別式を D として

$$\begin{aligned} \boldsymbol{D} &= \boldsymbol{(y+4)^2 - 4\cdot(3y^2 - 5y - 6)} \\ &= \boldsymbol{-11y^2 + 28y + 40 \geqq 0} \\ \therefore\ & \boldsymbol{11y^2 - 28y - 40 \leqq 0} \\ \therefore\ & \underbrace{\frac{14 - \sqrt{(14)^2 + 11\cdot 40}}{11}}_{(-)} \leqq y \leqq \underbrace{\frac{14 + \sqrt{(14)^2 + 11\cdot 40}}{11}}_{A} \cdots\cdots ② \end{aligned}$$

ここで A の部分を計算するのだが、$14^2 = 196,\ \ 25^2 = 625$ などはよく出てくるから、目見当にするとよい．

$$A = \frac{14 + \sqrt{636}}{11} = 3.5\cdots$$

ゆえに、② を満たす正整数 y の値は $y = 1,\ 2,\ 3$ である．

これらを ① に入れて

$$\begin{aligned} &y = 1 \longrightarrow x^2 - 5x - 8 = 0 \quad \text{整数解なし} \\ &y = 2 \longrightarrow x^2 - 6x - 4 = 0 \quad \text{整数解なし} \\ &y = 3 \longrightarrow x^2 - 7x + 6 = 0 \quad \therefore\ (x-1)(x-6) = 0 \quad \therefore\ x = 1,\ 6 \end{aligned}$$

で、結局、求める整数解は 2 組あって

$$(x,\ y) = (1,\ 3),\ \ (6,\ 3)$$

である．

★ $\boldsymbol{25^2 = 625}$ **など**

「 覚えておけ 」とは言わないが．筆者はいま

$$11^2 = 121,\quad 12^2 = 144,\quad 13^2 = 169,\quad 14^2 = 196,\quad 15^2 = 225,\quad 16^2 = 256$$

までは思い出すことができた．そのあとは忘れたが、なぜか $25^2 = 625$ は覚えていた．

(2) これも同様に x について整理すると

$$4x^2-2(y+6)x+(5y+11)=0 \cdots\cdots ①$$

この判別式を D とすると

$$\frac{D}{4}=(y+6)^2-4(5y+11)=y^2-8y-8$$

だが、$D \geqq 0$ からは $y \geqq 8.8\cdots$ となり、範囲が外に開いてしまって、(1) のように y の範囲を絞れない——別の方法を考えなければならない．そこでどうするか．

改めて ① を**解の公式**で解くと

$$x=\frac{y+6\pm\sqrt{y^2-8y-8}}{4} \cdots\cdots (*)$$

これが整数であるためには、とりあえずルート $\sqrt{(\cdots)}$ がはずれる、つまり、「 ルートの中が **完全平方数** $(\cdots)^2$ の形になる 」ことが必要である——ただし、これで十分とはいえない．

そこで

$$\frac{D}{4}=\boldsymbol{y^2-8y-8=N^2} \cdots\cdots ②$$

$$\longleftarrow \sqrt{(\cdots)}=N \text{ とおいた！}$$

結局、これを満たす y の正整数値を見つけて、① に入れて x の正整数値を拾う．つまり、不定方程式 ① をいきなり解く代わりに、必要条件として**不定方程式** ② 解く、と考えればよい．

さて ② だが、解き方の方法としては未知数をを含む部分を「 **積の形** 」に変えられないか．

② ： $(y-4)^2-16-8=N^2$

$\therefore$ $\boldsymbol{(y-4)^2-N^2=24}$ $\longleftarrow$ **平方数の差になる** ところがポイント！

$\therefore$ $\{(y-4)+N\}\{(y-4)-N\}=24 \cdots\cdots ③$

ここで、ハナシの途中だが、「 左辺の **2 つの因数**にかかわるハナシ 」を確認しておく．

$$\boxed{\boldsymbol{A^2-B^2=(A+B)(A-B)} \longleftarrow \boldsymbol{A+B} \text{ と } \boldsymbol{A-B} \text{ の偶奇が一致する！}}$$

つまり、$A,\ B$ の偶数と奇数で場合を分けて考えると

$\boldsymbol{A,\ B}$ **がともに偶数、またはともに奇数** $\longrightarrow$ $\boldsymbol{A+B}$ **と** $\boldsymbol{A-B}$ **はともに偶数！**

$\boldsymbol{A,\ B}$ **のどちらか一方が偶数、他方が奇数** $\longrightarrow$ $\boldsymbol{A+B}$ **と** $\boldsymbol{A-B}$ **はともに奇数！**

であるから、③ からわかることを整理すると

(i) 右辺の 24(偶数) から、$(y-4)+N$ と $(y-4)-N$ はともに偶数．

(ii) $(y-4)+N \geqq (y-4)-N$ （ $\because$ $N \geqq 0$ ）

(iii) $y \geqq 1,\ N \geqq 0$ より $(y-4)+N \geqq -3$

以上のことを考慮した上で、③ の右辺の 24 を 2 つの積に分解してみると

$y-4+N$	12	6	-2
$y-4-N$	2	4	-12

$\therefore$

$y+N$	16	10	2
$y-N$	6	8	-8

これらの中で適する $y,\ N$ の値は

$(y,\ N)=(11,\ 5),\ (9,\ 1)$ $\quad\therefore$ $(x,\ y)=(3,\ 11),\ (4,\ 9)$ （ $\because$ ②, $(*)$ ）

★ **整式を扱う基本——最低次の文字で整理してみる．**

与えられた**不定方程式**は

$$2xy-4x^2+12x-5y=11$$

この**左辺**は「 $\boldsymbol{y}$ **について 1 次式** 」ではないか――そういうときは、y について整理する．つまり、y について解いて解いてみる――この方法はすでに述べた．

$$(2x-5)y = 4x^2 - 12x + 11 \longleftarrow \boldsymbol{2x-5} \text{ は奇数だから } \mathbf{0} \text{ でない！}$$

$$\therefore \quad y = \frac{4x^2-12x+11}{2x-5} \longleftarrow \text{割り落とす！}$$

$$= \boldsymbol{2x - 1 + \frac{6}{2x-5}}$$

ここで、$2x-5$ は 6 の奇数の約数で $\pm 1,\ \pm 3$ が考えられるが、上記で

$$4x^2 - 12x + 11 = (2x-3)^2 + 2 > 0, \quad y > 0$$

だから、$2x-5>0$ でなければならない．そこで

$$2x - 5 = 1,\ \ 3 \qquad \therefore \quad x = 3,\ \ 4$$

これらに対して、それぞれ $y = 11,\ \ 9$ が決まるので

$$(x,\ y) = (3,\ 11),\ \ (4,\ \ 9)$$

となる――もちろん、これでもよい．むしろ、これが自然かも知れない．

＜ end. ＞

2.1.2.3　いろいろな方程式

われわれの扱える不定方程式の代表的なものは、ここまでで大体は述べたが、「 それにもれたもの 」もないわけではない———しかし、そう多くはない.

＜メモ＞

■ いろいろな方程式

典型的な形からもれたとはいえ、それでも「 あるカタチ 」の扱い方として括れるものもある．思いつくものをあげておく．

＜ 例 1 ＞

$xyz = x + y + z$ の正整数解を求めよ．

(解) 与えられた方程式は

$$xyz = x + y + z \quad \cdots\cdots ①$$

だが、この特徴は $x,\ y,\ z$ の**対称式**である．こういうときは「 **先に大小関係を決めておく** 」とよい．そこで、とりあえず

$$\boldsymbol{x \geqq y \geqq z \geqq 1} \quad \cdots\cdots ②$$

としてみると

$$3x \geqq x + y + z = xyz \qquad \therefore\ \ 3x \geqq xyz \qquad \therefore\ \ yz \leqq 3 \quad (\because\ \ x \geqq 1)$$

ここで、$y,\ z$ が正整数で ② を満たすことから $yz = 3,\ 2,\ 1$ で

y	3	2	1
z	1	1	1

これらの y, z の値から ① を満たす x を求めると

$$x \cdot 3 = x + 3 + 1 \qquad \therefore\ \ x = 2 \qquad (\ \times\ )$$
$$x \cdot 2 = x + 2 + 1 \qquad \therefore\ \ x = 3 \qquad (\ \bigcirc\ )$$
$$x \cdot 1 = x + 1 + 1 \qquad \therefore\ \ 0 = 2 \qquad (\ \times\ )$$

で結局、$(x,\ y,\ z) = (3,\ 2,\ 1)$ だが、大小関係 ② は問題の条件ではないので、「 その順序を入れかえた次の 6 組 」が求める解である．すなわち解は

x	3	3	2	2	1	1
y	2	1	3	1	3	2
z	1	2	1	3	2	3

となる．

＜ end. ＞

＜ 例 2 ＞

$x,\ y,\ z$ は、いずれも 1 より大きい整数で、x と y は互いに素である．このとき

$$z = (6y + 5x)\left(\frac{1}{y} - \frac{1}{x}\right)$$

を満たす $x,\ y,\ z$ を求めよ．

(解) まず、与えられた z を、「 因数の関係をつかむ 」ために

$$z = \frac{(6y + 5x)(x - y)}{xy} \quad \cdots\cdots ①$$

と変形しておく．

そうすると、「 **$x,\ y$ が互いに素だから、$x - y$ と xy も互いに素** 」がいえて、したがって x も y も $6y + 5x$ の約数でなければならない．そこで

$$\frac{6y + 5x}{x} = 5 + \frac{6y}{x}, \qquad \frac{6y + 5x}{y} = 6 + \frac{5x}{y}$$

は整数で、x と y は互いに素であるから、x は 6 の約数で、y は 5 の約数でなくてはならない．

ここで $x>1,\ y>1$ の条件を考慮して

$$x=2,\ 3,\ 6,\quad y=5$$

また、① で $z>0$ とすると $x>y$ だから

$$x=6,\quad y=5 \quad \therefore\quad z=2 \quad \longleftarrow\ x,\ y \text{ の値を①に代入！}$$

が得られる.

＜ end. ＞

＜ 例 3 ＞

次の連立方程式を満たす $x,\ y$ の正整数値を求めよ.

$$\begin{cases} x^3-y^3-z^3=3xyz \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ① \\ x^2=2(y+z)\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ② \end{cases}$$

(解) まず ① をもう少し「 よいカタチ 」に変形できないか.

$$x^3+(-y)^3+(-z)^3-3x(-y)(-z)=0 \ \longleftarrow\ \text{因数分解できる！}$$

ここで因数分解の公式

$$\boxed{\boldsymbol{a^3+b^3+c^3-3abc=(a+b+c)\ (a^2+b^2+c^2-bc-ca-ab)}}$$

を思い出してもらいたい———**コケオドシ**だった.

すなわち、上記の左辺は因数分解されて

$$\{x+(-y)+(-z)\}\{x^2+(-y)^2+(-z)^2-(-y)(-z)-(-z)x-x(-y)\}=0$$

$$\therefore\quad (x-y-z)\underbrace{(x^2+y^2+z^2-yz+zx+xy)}_{A}=0\cdots\cdots\cdots\cdots ③$$

ここで A の部分は

$$A=\frac{1}{2}\{(x+y)^2+(y-z)^2+(z+x)^2\}>0 \ \longleftarrow\ x,\ y,\ z \text{ は正整数！}$$

だから、これを ③ に適用すると

$$x-y-z=0 \quad \therefore\quad x=y+z\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ④$$

これを ② に入れると

$$x^2=2x \quad \therefore\quad x(x-2)=0 \quad \therefore\quad x=2\ \ (\ >0\ )$$

これを ④ に入れると

$$y+z=2$$

$y,\ z$ は正整数だから $y=z=1$ ゆえに、$x,\ y,\ z$ は

$$(x,\ y,\ z)=(2,\ 1,\ 1)$$

である.

＜ end. ＞

2.1.3　不等式の整数解

ついでに、不等式の場合もやっておく．これは、たとえば

$$f(x, y) > 0$$

のようなカタチで与えられる場合が多いが、こういうときは「 xy 平面上の領域の問題 」としてとらえると「 見通し 」がよくなることが多い．

＜メモ＞

■ 改めて、不等式の整数解

＜ 例 1 ＞

次の不等式を同時に満たす $x,\ y$ の整数値の組を求めよ．

$$1 < x + 5y < 5 \cdots\cdots\cdots\cdots ①, \qquad -1 < 2x + 7y < 3 \cdots\cdots\cdots\cdots ②$$

(解) ①, ② の表す領域を xy 平面上に図示しておく．そのために

$$x + 5y = 1,\ \ x + 5y = 5,\ \ 2x + 7y = -1,\ \ 2x + 7y = 3$$

の交点を求めて、図のように A, B, C, D とするとその座標は

$$\mathrm{A}\ \left(-\frac{40}{3},\ \frac{11}{3}\right),\ \ \mathrm{B}\ (-4,\ 1),\ \ \mathrm{C}\ \left(\frac{8}{3},\ -\frac{1}{3}\right),\ \ \mathrm{D}\ \left(-\frac{20}{3},\ \frac{7}{3}\right)$$

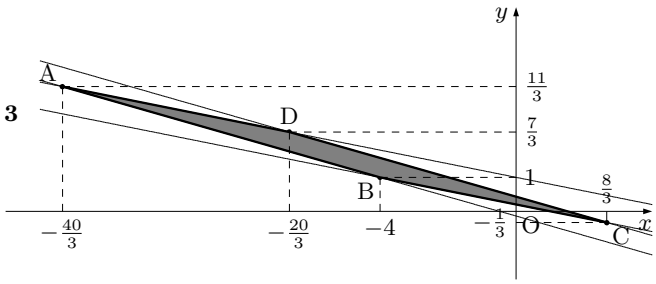
で、①② を満たす領域は、図の平行四辺形の内部になる．したがって、①② を満たす x, y の整数値の組は、この斜線部分の**格子点**を調べればよい．

そこで、この領域内にある点の y 座標の範囲は

$$-\frac{1}{3} < y < \frac{11}{3}$$

$$\longrightarrow\ \boldsymbol{y = 0,\ 1,\ 2,\ 3}$$

であるから、これらの y の値に対して、①② を満たす x の値を求めるのだが



$\boldsymbol{y = 0}$ のとき

$$\begin{cases} ①\ :\quad 1 < x < 5 \\ ②\ :\quad -\dfrac{1}{2} < x < \dfrac{3}{2} \end{cases} \longrightarrow \text{同時に満たす整数値はない！}$$

$\boldsymbol{y = 1}$ のとき

$$\begin{cases} ①\ :\quad -4 < x < 0 \\ ②\ :\quad -4 < x < -2 \end{cases} \longrightarrow x = -3$$

$\boldsymbol{y = 2}$ のとき

$$\begin{cases} ①\ :\quad -9 < x < -5 \\ ②\ :\quad -\dfrac{15}{2} < x < -\dfrac{11}{2} \end{cases} \longrightarrow x = -7,\ -6$$

$\boldsymbol{y = 3}$ のとき

$$\begin{cases} ①\ :\quad -14 < x < -10 \\ ②\ :\quad -11 < x < -9 \end{cases} \longrightarrow \text{同時に満たす整数値なし！}$$

以上より、求める $x,\ y$ の組は

$$(x,\ y) = (-3, 1),\ \ (-6, 2),\ \ (-7, 2)$$

である．

★ 格子点

$x,\ y$ がともに整数であるような点 $(x,\ y)$ を**格子点**という．

＜ end. ＞

＜例 **2**＞

不等式 $ab+1 \leqq abc \leqq bc+ca+ab+1$ を満たす自然数 $a,\ b,\ c$ のすべてを求めよ．ただし、$a>b>c$ とする．

(解) さて、どこから手をつけるか――どうもやりにくい．

それでもよく見ると、与えられた不等式は a と b をいれかえても変わらない**対称式**である．そこで、その「 **仲間はずれ**になっている c を中心に整理 」してみる．

$$ab+1 \leqq abc \ \longrightarrow ab(c-1) \geqq 1 \ \cdots\cdots ①$$
$$abc \leqq bc+ca+ab+1 \ \longrightarrow \ (ab-a-b)c \leqq ab+1 \cdots\cdots ②$$

ところで、$a,\ b,\ c$ は自然数だから ① より

$$c-1 \geqq 1 \quad \therefore \ c \geqq 2 \ \cdots\cdots ③$$

ここで、② の c の係数である $(ab-a-b)$ に注目すると

$$ab-a-b=(a-1)(b-1)-1>0 \quad (\ \longleftarrow \ a>b>c \geqq 2 \quad \therefore \ a>b \geqq 3\ )$$

ゆえに、c と 2 との大小関係から

$$\underbrace{2(ab-a-b)}_{A} \leqq (ab-a-b)c \leqq \underbrace{ab+1}_{B}$$

この大小関係の $A \leqq B$ を使う．すなわち

$$2(ab-a-b) \leqq ab+1 \quad \therefore \ ab-2a-2b \leqq 1$$
$$\therefore \ ab-2a-2b+4 \leqq 5 \quad \therefore \ \underbrace{(a-2)(b-2)}_{C} \leqq 5$$

ここで、可能性は $C=0,\ 1,\ 2,\ 3,\ 4,\ 5$ だが、$a>b \geqq 3$ であったから

$$a-2>b-2 \geqq 1$$

を考慮して

$a-2$	2	3	4	5
$b-2$	1	1	1	1

だが、$b=3$ だから $c=2$ と決まり、求める $a,\ b,\ c$ の組は

a	4	5	6	7
b	3	3	3	3
c	2	2	2	2

である．

＜ end. ＞

2.2　その他についての発展的考察

2.2.1　ペル方程式

ペル方程式というのは

$$\boldsymbol{x^2 - Dy^2 = 1 \quad (D \text{ は整数})} \cdots\cdots ①$$

の形をした**不定方程式**のことである．ただし、正確には右辺は ± 1 だが、ここでは 1 の場合で説明することにする．

もともと、これは不定方程式のファミリーではあるが、実際の入試では整数解を求めるというだけでなく、もう少しちがう角度からの問いかけであったりするので別に紙面を用意した．ここではそういう視点からの解説も試みようと思う．

2.2.1.1　解集合の構造

さて、改めてペル方程式 ① をながめてみると、$y = 0$ なら D にかかわらず $x = \pm 1$ であるが、これは別ワクとしておく．そうすると $D > 0,\ D = 0,\ D < 0$ の場合を調べることになるが、手近のところから行くと次のように分類されそうだ．

(i)　$D = 0$ のとき：$x = \pm 1,\ y$ は任意の整数

(ii) $D = -1$ のとき：$x = 0,\ y = \pm 1$

(iii) $D < -1$ のとき：$x = \pm 1,\ y = 0$

(iv) $D = a^2$ (完全平方数) のとき：

$$x^2 - a^2y^2 = (x + ay)(x - ay) = 1$$

$$\therefore \quad \begin{cases} x + ay = \pm 1 \\ x - ay = \pm 1 \end{cases} \quad \longrightarrow \quad x = \pm 1,\ y = 0 \quad (\text{複合同順})$$

(v)　上記以外の場合：<u>$D > 0$ で、D が完全平方数でない</u>

で、<u>結局、(v) **の場合の検証**がテーマ</u> ということになる．

そこで D に具体的な数値、たとえば $D = 3$ を与えると

$$x^2 - 3y^2 = 1 \cdots\cdots ②$$

$$\therefore \quad (x + \sqrt{3}y)(x - \sqrt{3}y) = 1 \cdots\cdots ③$$

ここで $x + \sqrt{3}y = X,\ x - \sqrt{3}y = \overline{X}$ とおく——複素数の共役の関係と対応させて考える．そうすると ③ では積の交換則も成り立つから

$$X\overline{X} = \overline{X}X = 1 \cdots\cdots ④$$

である——さて、準備はできた．

いま、ペル方程式 ② の解 (x, y) に対して $x + y\sqrt{3}$ (x, y は整数) で構成される集合を K とする——これをペル方程式 ② の**解集合**と呼ぶことにする．

$$\boldsymbol{K = \{x + y\sqrt{3} \mid x^2 - 3y^2 = 1,\ \text{ただし } x, y \text{ は整数}\}}$$

のことだが、この解集合にはおもしろい性質がある．以下に列挙する．

(1) $\boldsymbol{\alpha \in K,\ \beta \in K}$ **ならば** $\boldsymbol{\alpha\beta \in K}$ **である**———K は積に関して閉じている．

なぜなら、④ に示すように

$$\left.\begin{array}{l} \alpha \in K \ \longrightarrow\ \alpha\overline{\alpha} = 1 \\ \beta \in K \ \longrightarrow\ \beta\overline{\beta} = 1 \end{array}\right\} \qquad \therefore\ \ (\alpha\beta)(\overline{\alpha\beta}) = (\underbrace{\alpha\overline{\alpha}}_{1})(\underbrace{\beta\overline{\beta}}_{1}) = 1$$

となるからである．

(2) $\boldsymbol{\alpha, \beta, \gamma \in K}$ **のとき** $\boldsymbol{\alpha(\beta\gamma) = (\alpha\beta)\gamma}$ ———**結合則**が成り立つ．

(3) 単位元がある．

$x = 1,\ y = 0$ は ③ の解、すなわち $1 \in K$ であるから、任意の要素 $\alpha \in K$ に対して

$$\alpha e = \alpha \ \longleftarrow\ e = 1$$

となる要素である**単位元** $\boldsymbol{e \in K}$ がある．

(4) 逆元がある．

$\alpha \in K$ ならば $\boldsymbol{\alpha\phi = 1}$ **(1 は単位元** $\boldsymbol{e}$**)** となる $\phi \in K$ がある．なぜなら $\alpha\overline{\alpha} = 1$ から $\alpha \in K$ ならば、つねに $\overline{\alpha} \in K$ である．すなわち

$$\overline{\alpha} = \frac{1}{\alpha} = \alpha^{-1}\ (= \phi)$$

が α の逆元 ϕ である．

以上の考察により、<u>K は積に関して**群**をなす</u> ことがわかる．しかも

$$\alpha\beta = \beta\alpha\ \ (\alpha,\ \beta \in K)\ \longleftarrow\ \text{交換則成立！}$$

が成り立つから**アーベル群** (**可換群**) であることがわかる．

(注) **群について**

群 (**ぐん**) とは何か———難しいハナシをするつもりはないが、チョッと知っていれば何かのときに役に立つかも知れない．まあ、今のところそんなものかと思ってもらえばよい．

かつて高校数学でも、**行列と 1 次変換** が始めて導入されたときは、確か高校の教科書に載っていたのだが、いつの間にかなくなってしまったので、改めて本文の (1)〜(5) ながめてもらいたい．

たとえば、行列の例で説明すると

$$AX = B\ \longleftarrow\ A,\ B,\ X \text{ は } 2 \times 2 \text{ 行列とする！}$$

を満たす X を求める場合、<u>行列では割り算ができない</u> から $X = \dfrac{B}{A}$ とやることはできない．

しかし、左辺の A に工夫をして何とかこの方程式を $X = (\cdots)$ と同値変形したい．そこで、行列 A に左からかけて、本文 (3) の**単位元** $\boldsymbol{E}$**(単位行列)** なるような行列を作ろうというワケだ．

そういう、(4) でいう**逆元** $\boldsymbol{A^{-1}}$**(逆行列)** が作れれば、上の方程式に左からかけて

$$\underbrace{A^{-1}A}_{E}X = A^{-1}B \qquad \therefore\ \ X = A^{-1}B$$

として目的を達成することができる．

<u>行列の積は可換ではない</u> ので、次のような場合は右からかけることで実現できる．すなわち

$$XA = B \qquad \therefore\ \ X\underbrace{AA^{-1}}_{E} = BA^{-1} \qquad \therefore\ \ X = BA^{-1}$$

である———このように説明すると、何か特別に難しいことをしているように感じるかも知れないが、次の例を見てもらいたい．

$$5x = 3 \qquad \therefore\ \ x = \frac{3}{5}$$

という、昔からやっているあたりまえの計算を何気に書いたが、これを先の行列の例に倣って分解してみよう．

まず左辺の $5x$ の係数 5 を何とかしたい———左辺の係数を **単位元 1** にするために、両辺に **5 の 逆元 $\frac{1}{5}$** をかける、として書き換えると

$$5x = 3 \longrightarrow \underbrace{\frac{1}{5} \times 5}_{1}\ x = \frac{1}{5} \times 3 \qquad \therefore\ \ x = \frac{3}{5}$$

と 読むことができる．つまり、行列の例も数値計算の例も、本文 (1)〜(4) の**構造**をもつ集合の要素と要素の間の**演算**として構成することができる．

このような数学の分野を**構造的代数学**と呼んだりしているが、これは数学の 1 つの分野というより、**集合論**と併せて数学のあらゆる分野にかかわっていると考えた方がよい．

さて、改めて群とは何か．本文の (1)〜(4) をカンタンに表すと、「群とはある**演算**ができて、その**逆演算**ができる集合」ということ で、**可換群**というのはその演算が交換可能の場合のことである．

さて、せっかくここまで書いたから、ついでに**環 (かん)** と**体 (たい)** にもチョッとだけ触れておきたい．と言っても、詳細には自分で勉強してもらうとして、ここでは「おおむねこんなことだ」という程度のザックリとした説明ではあります．

環というのは、次のような 2 種類の結合、$+$ と $\times$ をもつ集合のことである．

(i) $+$ については**可換群**をなす $\longrightarrow$ $a + b = b + a,\quad (a + b) + c = a + (b + c)$

また、任意の a で $a + 0 = a$ から**単位元**は 0、**逆元**を $-a$ で表して $a + (-a) = 0$ である．

(ii) $\times$ については**結合則**が成り立つ $\longrightarrow$ $(ab)c = a(bc)$

(iii) $+$ と $\times$ の間には**分配則**が成り立つ $\longrightarrow$ $a(b + c) = ab + ac,\ (a + b)c = ac + bc$

つまり、1 つの演算 $+$ とその逆演算 $-$ が定義できて、もう 1 つの演算 $\times$ が定義できるがその逆演算 $\div$ が定義できない集合のことで、例としては**整数の集合**などが挙げられる．

次に**体**だが、まず**環**であって、しかも 0 以外の要素が乗法ついて**群**を構成するとき、その集合を体といい、その乗法の単位元を e で表す．その例としては、実数全体のつくる環である**実数体**、複素数全体の**複素数体**などを思い浮かべればよい．

以上、予定外の余計なことまで書いてしまった．本気で深入りすることはないが、知っていてジャマになるほどのものでもない．

(注) ＜ end ＞

＜補足説明！＞

ペル方程式の一般的な解法は西洋では**ウイリアム・ブランカー**という人が発見した．ところが、オイラーはこの方程式を研究したのはジョン・ペルであると**誤解**して「ペル方程式」と命名したため、以来その名前が広く使われるようになったといわれている．

しかし、このテーマについてはインドなどではその 1000 年も前に研究されていたともいわれていて、昔から人々が興味をもっていたらしいことはうかがい知ることができる．

21 世紀に生きるわれわれとしては「どうでもよい」といえばそれまでだが、パソコンもテレビもない時代に、というより そういう時代であったからこそ かも知れないが、こういうテーマに集中した人々がいたことに改めて驚き、何かしら暖かいものを感じるのは筆者だけではないと思う．まあ、遊びのつもりで堪能して下さい．

＜ end.＞

2.2.1.2　整数解を求める

われわれとしてはペル方程式 ② の整数解を求めるのが目的だが、その解のうち x, または y が 0 のものは $(\pm 1,\ 0)$ だけであるから、とりあえずこれは除いておくことにする——議論を進める上でそれなりの理由があるのです.

そうすると $xy \neq 0$ (つまり、いずれも 0 でない) である解の 1 つを $(x,\ y)$ とすると $(x,\ -y)$, $(-x,\ y)$, $(-x,\ -y)$ も解になる. そういうことなら、まず x, y がともに正のものに限って調べればよいことになる.

ところでこの場合、ペル方程式は

$$\boldsymbol{x^2 - 3y^2 = 1} \cdots\cdots ①$$

$$\therefore\ \ (x+\sqrt{3}y)(x-\sqrt{3}y) = X\overline{X} = 1$$

だから、この解のうち x, y がともに正のもの、すなわち

$$\boldsymbol{X = x + \sqrt{3}y\ \ (x > 0,\ y > 0)} \cdots\cdots ②$$

で構成される集合を $\boldsymbol{K_0}$ と表して考察を進めることにする.

いま、K_0 の要素を α, β とすると、K_0 は積については閉じている、すなわち

$$\left.\begin{array}{l}\alpha \in K_0 \\ \beta \in K_0\end{array}\right\} \longrightarrow \alpha\beta \in K_0 \qquad \therefore\ \ \alpha^2 \in K_0 \quad (\ \longleftarrow\ \beta\text{を}\alpha\text{とおいた！})$$

である. これを繰り返していくと α, α^2, α^3, $\cdots\cdots\cdots$ はすべて K_0 の要素になることがわかる. このことから、α をうまく選んで K_0 の すべて要素を αの累乗 (α^p) の形 で表すことはできないか——実は**デキル**のです.

さて、上記の K_0 の要素の 1 つ $X = x + \sqrt{3}y$ (x, y は正整数) とおくと

$$x^2 - 3y^2 = 1 \ \longrightarrow\ x = \sqrt{3y^2+1}\ \ (\because x > 0)$$

$$\therefore\ \ X = \sqrt{3y^2+1} + \sqrt{3}y \cdots\cdots (*)$$

だが、この $\boldsymbol{X}$ は $\boldsymbol{y \geqq 0}$ **の範囲で** $\boldsymbol{y}$ **の増加関数**になっている.

つまり、y の大小によって X の大小が決まり、y は正整数だから X には**最小のもの**があり、それを α とすると K_0 の要素は α の累乗 (α^p) の形 で表される らしい.

つまり、$y = 1,\ 2,\ \cdots\cdots\cdots$ に対して x が整数になるものを拾っていけば順次

$$y = 1 \ \longrightarrow\ X_1 = 2 + \sqrt{3} = \alpha$$

$$y = 4 \ \longrightarrow\ X_2 = 7 + 2\sqrt{3} = (2+\sqrt{3})^2 = \alpha^2$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\cdots\cdots\cdots\cdots\cdots$$

のようになるだろう.

かくして、適当な正整数 y_n に対してそれに対応する正整数 x_n が定まり

$$X_n = x_n + y_n\sqrt{3} \ \longleftarrow\ \ x_n,\ y_n\text{は正整数！}$$

$$= (2+\sqrt{3})^n = \alpha^n$$

となりそうだ——まあ、これでソレらしい予想はできる.

しかし、十分にナットクして使うにはもう少しキチンとしなければなるまい. それには次の 2 つの要件についての説明が求められる. つまり、それで解集合 K_0 のすべてを尽くしているか ということである.

＜1＞ $\underline{\boldsymbol{(2+\sqrt{3})^n}}$ **の形のものはすべて ペル方程式 ①の解集合か.**

まず、$(2+\sqrt{3})^n$ の形をした任意の要素が $x_n+y_n\sqrt{3}$ (x_n, y_nは正整数) の形で表され、この正整数 x, y の部分がペル方程式 ① を満たすことをいう——**数学的帰納法**でやっておこう.

(i) $n=1$ のとき

$$(2+\sqrt{3})^1 = 2+1\cdot\sqrt{3} \quad \therefore\ x_1=2,\ y_1=1 \ \longleftarrow\ x_1,\ y_1\text{は正整数！}$$
$$\therefore\ x_1^2-3y_1^2=2^2-3\cdot 1^2=1 \ \longleftarrow\ \text{ペル方程式を満たす！}$$

(ii) $n=k$ のとき成立すると仮定すれば

$$(2+\sqrt{3})^k = x_k+y_k\sqrt{3} \quad \longleftarrow\ x_k,\ y_k\text{は正整数！} \quad \cdots\cdots\cdots\cdots(**)$$
$$x_k^2-3y_k^2=1 \quad \longleftarrow\ \text{ペル方程式を満たす！}\cdots\cdots\cdots\cdots\cdots\cdots(***)$$

このとき

$$\begin{aligned}(2+\sqrt{3})^{k+1} &= (2+\sqrt{3})^k(2+\sqrt{3}) \quad \longleftarrow\ (**)\\ &= (x_k+y_k\sqrt{3})(2+\sqrt{3})\\ &= \underbrace{(2x_k+3y_k)}_{x_{k+1}\text{とおく}}+\underbrace{(x_k+2y_k)}_{y_{k+1}\text{とおく}}\sqrt{3} = x_{k+1}+y_{k+1}\sqrt{3}\end{aligned}$$

$x_k,\ y_k$ がともに正整数だから $\underline{x_{k+1},\ y_{k+1}\ \text{はともに正整数である}}$.

さらに、$x_{k+1},\ y_{k+1}$ を ① の左辺に代入してみると

$$\begin{aligned}x_{k+1}^2-3y_{k+1}^2 &= (2x_k+3y_k)^2-3(x_k+2y_k)^2\\ &= x_k^2-3y_k^2=1 \quad \longleftarrow\ (***)\end{aligned}$$

で、ペル方程式も満たしている.

すなわち、(i)(ii) から条件は示された．つまり

$$\boldsymbol{(2+\sqrt{3})^n = x_n+y_n\sqrt{3}\ (x_n, y_n\text{は正整数})}$$

の x_n, y_n はすべて**ペル方程式** ① の正整数の解である.

＜2＞ $\underline{\boldsymbol{K_0}}$**に** $\boldsymbol{(2+\sqrt{3})^n}$ **の形 以外の解はないか.**

これは $(2+\sqrt{3})^n$ の形 で条件の解集合 K_0 の要素すべてを尽くしているか ということであるが、チョッと難しいので注意して読み進めてもらいたい.

さて、K_0 の**最小の要素**が $\alpha=2+\sqrt{3}>1$ であるから

$$1<\alpha<\alpha^2<\alpha^3<\cdots\cdots\alpha^n\cdots\cdots\cdots$$

で、このとき、K_0 の**任意の要素を** $\boldsymbol{\beta}$ とすると

$$\alpha^n \leqq \beta < \alpha^{n+1} \ \longleftarrow\ \beta=x+y\sqrt{3}\ \ (x,\ y\ \text{は正整数}),\ x^2-3y^2=1$$

とおくことができる——そのような n が必ず存在するはず！

そこで、$\alpha^n>0$ で不等式の各辺を割ると

$$\boldsymbol{1 \leqq \frac{\beta}{\alpha^n} < \alpha}\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(****)$$

ここで、先の**解集合の構造**で述べた集合 $\boldsymbol{K}$ を思い出してもらいたい．ここでは

$$\boldsymbol{K = \{x + y\sqrt{3} \mid x^2 - 3y^2 = 1,\ \text{ただし}\ x, y\ \text{は整数}\}}$$

として K_0 での $\boldsymbol{x, y}$ **は正整数** というシバリがはずれている．つまり

$$\left.\begin{array}{lll} \alpha \in K & \therefore\ \overline{\alpha} \in K & \therefore\ \overline{\alpha}^n \in K \\ \beta \in K & & \end{array}\right\} \quad \therefore\ \beta\overline{\alpha}^n = \frac{\beta}{\alpha^n} \in K$$

で、結局 $\beta\overline{\alpha}^n$ は $\alpha = 2 + \sqrt{3}$ が最小の要素である K_0 の要素ではないが、$x > 0,\ y > 0$ というシバリのない**ペル方程式**の解集合 K の要素であることがわかる．

そこで、改めて $(*)$ を思い出そう．つまり

$$\begin{aligned} \beta\overline{\alpha}^n &= x + y\sqrt{3} \longleftarrow\ x^2 - 3y^2 = 1 \\ &= \sqrt{3y^2 + 1} + y\sqrt{3} \\ &\quad \longleftarrow\ x = -\sqrt{y^2 + 3}\ \text{のときは}\ \beta\overline{\alpha}^n < 0\ \text{で}\ (****)\ \text{を満たさない！} \end{aligned}$$

しかも、これは $y \geqq 0$ で単調増加で $y = 1$ に対しては $2 + \sqrt{3}$ で $(****)$ を満たさない．

そこで、仕方がないから $x > 0$ の条件はそのまま、$y > 0$ というシバリを解いて、$y = 1$ より 1 小さい整数 $y = 0$ (このとき $x = 1$) を許すと $\beta\overline{\alpha}^n$ の値は

$$[\ \beta\overline{\alpha}^n\ ]_{y=0} = \sqrt{3 \cdot 0^2 + 1} + 0 \cdot \sqrt{3} = 1 \quad \longleftarrow\ (****)\ \text{を満たす！}$$

$$\therefore\ \boldsymbol{\frac{\beta}{\alpha^n} = \beta\overline{\alpha}^n = 1} \quad \therefore\ \boldsymbol{\beta = \alpha^n}$$

したがって、<u>K_0 の要素には α^n (累乗！) の形以外のものはない.</u>

すなわち、＜1＞＜2＞の考察によりペル方程式

$$x^2 - 3y^2 = 1\ (x > 0,\ y > 0)$$

の解集合 K_0 は α^n $(n = 1,\ 2,\ 3,\ \cdots\cdots\cdots)$ として

$$K_0 = \{\alpha,\ \alpha^2,\ \alpha^3,\ \cdots\cdots,\ \alpha^n,\ \cdots\cdots\cdots\} \longleftarrow\ \alpha = 2 + \sqrt{3}$$

であることが確定した．

そうすると、ペル方程式 ①の正整数解を $(x_n,\ y_n)$ として

$$\boldsymbol{x_n + \sqrt{3}y_n = \alpha^n\ \ (n = 1,\ 2,\ 3,\ \cdots\cdots\ )}$$

と表されることがわかる．しかし、$y = 0 \longrightarrow X_0 = 1 = \alpha^0$ も許して

$$\boldsymbol{x_n + \sqrt{3}y_n = \alpha^n\ \ (n = 0,\ 1,\ 3,\ \cdots\cdots\ )} \qquad \cdots\cdots\cdots\cdots\cdots ③$$

と表すときもある——漸化式で扱うときなどはこの方が自然に見える．

実際に、解 $x_n,\ y_n$ を具体的に求めるには、これらが **ペル方程式①** を満たすことから

$$x_n{}^2 - 3y_n{}^2 = 1 \quad \therefore\ (x_n + y_n\sqrt{3})(x_n - y_n\sqrt{3}) = 1$$

$$\begin{aligned} \therefore\quad x_n - y_n\sqrt{3} &= \frac{1}{x_n + y_n\sqrt{3}} \\ &= \frac{1}{(2 + \sqrt{3})^n} = (2 - \sqrt{3})^n = \overline{\alpha}^n \cdots\cdots\cdots\cdots\cdots ④ \end{aligned}$$

ここで ③＋④, ③－④ を計算すると

$$\begin{cases} x_n = \dfrac{\alpha^n + \overline{\alpha}^n}{2} = \dfrac{1}{2}\left\{(2+\sqrt{3})^n + (2-\sqrt{3})^n\right\} \\ y_n = \dfrac{\alpha^n - \overline{\alpha}^n}{2\sqrt{3}} = \dfrac{1}{2\sqrt{3}}\left\{(2+\sqrt{3})^n - (2-\sqrt{3})^n\right\} \end{cases} \qquad (n = 0,\ 1,\ 2,\ \cdots\cdots)$$

とすればよい.

これが正整数とは信じがたいカオをしているが、実は正整数なのです――なかなかおもしろい事実ではあります.

＜補足説明！＞

余談だが、**ペル方程式の解集合**のハナシは、あたかも複素数の**円分方程式**

$$\boldsymbol{z^n = 1} \ \longleftarrow\ \boldsymbol{z}\ \textbf{は複素数！}$$

の解

$$z = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \quad (\ k = 0,\ 1,\ 2,\ \cdots\cdots\cdots n-1)$$

のうち、$k = 0$ は 1 だからこれは除いて k の最小値 1 に対する

$$\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = \alpha \quad \longleftarrow \text{ 原始 } n \text{ 乗根という！}$$

をとり、その解集合全体を

$$\{\alpha^0,\ \alpha^1,\ \alpha^2,\ \cdots\cdots\cdots \alpha^{n-1}\}$$

と表すのと似ていておもしろい．機会があったらつき合せて較べてみるとよい.

＜ end.＞

＜メモ＞

■ ペル方程式と入試問題

ペル方程式の骨子については本文で説明したが、これはなかなか応用範囲が広くてきわめて重要なテーマである．しかし、入試問題に見られるものは時間的な制限もあり、いくつかの基本的な性質や扱い方に限られるようである．

以下、本文の確認の意味もかねて、典型的なものを挙げておく．

＜ 例 1 ＞

数列 $\{x_n\}, \{y_n\}$ は

$$x_n + y_n\sqrt{2} = (3+2\sqrt{2})^n \ (n = 1, 2, 3, \cdots\cdots\cdots) \quad \cdots\cdots\cdots\cdots\cdots\cdots ①$$

を満たす整数の数列とする．

(1) $a + b\sqrt{2} = c + d\sqrt{2}$ ($a,\ b,\ c,\ d$ 整数) ならば $a = c,$ かつ $b = d$ であることを示せ．

(2) すべての n について $x_n - y_n\sqrt{2} = (3-2\sqrt{2})^n$ が成り立つことを示せ．

(3) すべての n について $x_n^2 - 2y_n^2 = 1$ が成り立つことを示せ．

(解) (1) このハナシはすでに**数の分類**で解説したから復習である．

$$a + b\sqrt{2} = c + d\sqrt{2} \ (a,\ b,\ c,\ d \text{ 整数}) \qquad \therefore \ (a-c) + (b-d)\sqrt{2} = 0$$

ここで $b \neq d$ とすると

$$\sqrt{2} = -\frac{a-c}{b-d} \ \longleftarrow \ \text{左辺は無理数、右辺は有理数で等号は成り立たない}$$

$$\therefore \ b = d \qquad \therefore \ a = c$$

(2) 与えられた条件式 ① から漸化式を作る．

$$\begin{aligned} x_{n+1} + y_{n+1}\sqrt{2} &= (3+2\sqrt{2})^{n+1} \\ &= (3+2\sqrt{2})(3+2\sqrt{2})^n \\ &= (3+2\sqrt{2})(x_n + y_n\sqrt{2}) \\ &= (\underbrace{3x_n + 4y_n}_{x_{n+1}}) + (\underbrace{2x_n + 3y_n}_{y_{n+1}})\sqrt{2} \end{aligned}$$

ここで (2) を用いて両辺を比較すると

$$\boldsymbol{x_{n+1} = 3x_n + 4y_n, \quad y_{n+1} = 2x_n + 3y_n} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (*)$$

であるから

$$\begin{aligned} x_{n+1} - y_{n+1}\sqrt{2} &= (3x_n + 4y_n) - (2x_n + 3y_n)\sqrt{2} \\ &= (3-2\sqrt{2})x_n - (3\sqrt{2}-4)y_n \\ &= (3-2\sqrt{2})(x_n - y_n\sqrt{2}) \end{aligned}$$

すなわち、数列 $\{x_n - y_n\sqrt{2}\}$ は初項 $x_1 - y_1\sqrt{2}$、 公比 $(3-2\sqrt{2})$ の等比数列である．つまり

$$\begin{aligned} x_n - y_n\sqrt{2} &= (3-2\sqrt{2})^{n-1}(x_1 - y_1\sqrt{2}) \ \longleftarrow \ ①\text{で } n=1 \text{ とおくと } x_1 = 3,\ y_1 = 2 \\ &= (3-2\sqrt{2})^n \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots ② \end{aligned}$$

となる———定型の**数学的帰納法**にしたがってやってもよいが、① を用いて誘導する**漸化式 (∗)** は避けられない．自分で書いて確かめておくとよい．

(3) ここまでくれば、もう説明するまでもない———①と② を辺々かけて

$$(x_n + y_n\sqrt{2})(x_n - y_n\sqrt{2}) = (3+2\sqrt{2})^n(3-2\sqrt{2})^n \qquad \therefore \ x_n^2 - 2y_n^2 = 1$$

を得る．

＜ end. ＞

＜例 **2**＞

双曲線

$$x^2-3y^2=1 \cdots\cdots ①$$

が与えられている．次のことを証明せよ．ただし $a,\ b$ を整数とする．

(1) 点 $(a,\ b)$ を双曲線 ① 上の点とするとき、点 $(2a+3b,\ a+2b)$ は ① 上にある．

(2) n を正整数として $a+b\sqrt{3}=(2+\sqrt{3})^n$ を満たす $a,\ b$ をとれば、点 $(a,\ b)$ は ① 上にある．

(解) (1) 点 $(2a+3b,\ a+2b)$ が ① 上にあることをいうのだから、とりあえず代入してみよう

$$(2a+3b)^2-3(a+2b)^2=a^2-3b^2=1$$

$$\longleftarrow \text{ 点 } (a,\ b) \text{ は①上だから } \boldsymbol{a^2-3b^2=1}$$

で、成り立ってしまった——点 $(2a+3b,\ a+2b)$ は ① 上にある！

(2) さて、こうなると何だかわからないが、実は <u>前問と同じ</u> なのです．とはいえ、**品格**がちがう．こういうものを入試問題というのだと筆者は思ってしまう．せいぜい堪能して下さい．

どういうことかというと、初見では何だかわからないにしても、$a=x_n,\ b=y_n$ とおいてみるとハナシはずっとカンタンになる．たとえば (1) は

$$2a+3b=2x_n+3y_n,\quad a+2b=x_n+2y_n$$

これを見ると、それぞれを $x_{n+1},\ y_{n+1}$ とおいてみたくならないか．

そうすると

$$\boldsymbol{x_{n+1}=2x_n+3y_n,\quad y_{n+1}=x_n+2y_n}$$

という漸化式ができて、(1) は双曲線 ① 上の点 P_n から P_{n+1} に対応する漸化式を与えていることになる．そこで、改めて与えられた条件を読み換えると

$$x_n+y_n\sqrt{3}=(2+\sqrt{3})^n \cdots\cdots ②$$

だから

$$\boldsymbol{x_n-y_n\sqrt{3}=(2-\sqrt{3})^n} \cdots\cdots ③$$

を作って辺々かければよいだろう．そうすると

$$(x_n+y_n\sqrt{3})(x_n-y_n\sqrt{3})=(2+\sqrt{3})^n(2-\sqrt{3})^n \longrightarrow \boldsymbol{x_n^2-3y_n^2=1}$$

になるにちがいない——これで一件落着だ．

そして、(1) は ② を作るためのものだろう．実際にやってみると

$$\begin{aligned} x_{n+1}-y_{n+1}\sqrt{3} &= \boldsymbol{(2x_n+3y_n)}-\boldsymbol{(x_n+2y_n)}\sqrt{3} \\ &= (2-\sqrt{3})x_n-(2-\sqrt{3})y_n\sqrt{3} \\ &= (2-\sqrt{3})(x_n-y_n\sqrt{3}) \end{aligned}$$

で、数列 $\{x_n-y_n\sqrt{3}\}$ が等比数列であることから ② が誘導されることになる．ただし、$x_1,\ y_1$ は与えられた条件 ② で $n=1$ とおいて決定する．

$$\begin{aligned} x_n-y_n\sqrt{3} &= (2-\sqrt{3})^{n-1}(x_1-y_1\sqrt{3}) \\ &= (2-\sqrt{3})^n \end{aligned}$$

さて、本問の解説はこんなとことでよいだろう．そこで、この解答を隠して <u>改めて問題だけを見てもらおう</u>——上に示したような解答が書けますか．

よほど上手に**問題の本質**をつかんでいないと咄嗟にこうはいかない．こういうところで本当の**実力**が問われるのだと思いますよ．

＜ end. ＞

＜例 **3**＞

2 つの条件

(i) $a^2-2b^2=1$, または $a^2-2b^2=-1$　　(ii) $a+\sqrt{2}b>0$

を満たす任意の整数 $a,\ b$ から得られる実数 $g=a+\sqrt{2}b$ 全体から得られる集合を G とする．
1 より大きい G の要素のうち最小のものを u とおく．
(1) g を求めよ．　(2) 整数 n と G の要素 g に対し、gu^n は G の要素であることを示せ．
(3) G の任意の要素 g は適当な整数 m によって $g=u^m$ と表されることを示せ．

(解)(1) $u=a+\sqrt{2}b$ とおくと、与えられた条件から

$$a^2-2b^2=(a+\sqrt{2}b)(a-\sqrt{2}b)=\pm1\ ,\ a+\sqrt{2}b>0$$

$$\therefore\quad u=a+\sqrt{2}b=\frac{1}{|a-\sqrt{2}b|}>1\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\text{①}$$

$$\therefore\quad |a-\sqrt{2}b|<1\qquad\therefore\quad -1<a-b\sqrt{2}<1$$

これと ① とで

$$\begin{cases}a-\sqrt{2}b>-1\\ a+\sqrt{2}b>1\end{cases}\qquad\therefore\quad 2a>0\quad\therefore\quad a>0$$

$$\begin{cases}\sqrt{2}b-a>-1\\ \sqrt{2}b+a>1\end{cases}\qquad\therefore\quad 2\sqrt{2}b>0\quad\therefore\quad b>0$$

ゆえに、$a+\sqrt{2}b$ が最小になるのは $a=b=1$、すなわち求めるものは $u=1+\sqrt{2}$ である．
(2) G における任意の 2 つの要素 $g,\ h$ を

$$g=a+\sqrt{2}b,\ h=c+\sqrt{2}d\quad(\text{ただし、}a,\ b,\ c,\ d,\ \text{は条件 (i), (ii) を満たす整数})$$

とおくと

$$gh=(\underbrace{a+\sqrt{2}b}_{(+)})(\underbrace{c+\sqrt{2}d}_{(+)})=(\underbrace{ac+2bd}_{A\ \text{とおく}})+\sqrt{2}(\underbrace{ad+bc}_{B\ \text{とおく}})>0$$

$$\begin{aligned}\therefore\quad A^2-2B^2&=(ac+2bd)^2-2(ad+bc)^2\\&=(a^2c^2+4b^2d^2)-2(a^2d^2+b^2c^2)=(a^2-2b^2)(c^2-2d^2)=\pm1\end{aligned}$$

が成り立つから $gh\in G$、つまり、G は積について閉じているから u^k(k は正整数) $\in G$ である．
次に u^{-k}(k は正整数) について考察する．

$$u^{-1}=\frac{1}{1+\sqrt{2}}=-1+\sqrt{2}\in G\ \longrightarrow\ u^{-k}=(u^{-1})^k\in G$$

また u^0 については

$$\begin{cases}u^k\ \ (k\ \text{は正整数})\in G\\ u^{-k}(k\ \text{は正整数})\in G\end{cases}\qquad\therefore\quad u^ku^{-k}=\frac{u^k}{u^k}=1=u^0\in G$$

ゆえに、u^n(n は任意の整数) $\in G$、また、$g\in G$ ならば当然 gu^n(n は任意の整数) $\in G$ である．
(3) g の任意の要素を v とすると、次の不等式を満たす整数 m が必ず存在する．
すなわち、u が G の 1 より大きい最小の要素であるから、1 以下の要素にも注目して

$$u^m\leqq v<u^{m+1}\qquad\therefore\quad\boldsymbol{1\leqq vu^{-m}<u}\ \longleftarrow\ vu^{-m}\in G\ (\ \longleftarrow\ v\in G,\ \ u^{-m}\in G\ )$$

$$\therefore\quad\boldsymbol{vu^{-m}=1}\qquad\therefore\quad v=u^m$$

＜ end. ＞