第1章　はじめに

1.1　不定方程式

中学校で2次方程式の解の公式を学び，整数や有理数でない数，すなわち無理数を導入し，さらに高校では，すべての2次方程式が解をもつように，数の範囲を複素数にまで広げていった． この講義では，素朴な立場に戻り，方程式の解の範囲を整数や有理数に限定して，解の存在やその解き方に着目してみよう．

たとえば，3次方程式

$$x^3 - 3x^2 + 5x - 6 = 0$$

を解くことを考える．高校の【数学II】では，解の候補として，定数項の約数 $\pm1, \pm2, \pm3, \pm6$ がとれることを学んだ． 実際，この場合 $x = 2$ が解であることが確かめられ，さらに整数解は $x = 2$ だけであることが確認できる． 一般の整数係数 n 次代数方程式

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0 \qquad (c_k \in \boldsymbol{Z},\ c_n \neq 0)$$

の整数解も，$c_n = 1$ のときには，定数項 c_0 の約数（それは有限個である）をチェックすればすべて得られる． $c_n \neq 1$ の場合も，この方法を少し修正すればすべての整数解を決定できる (考えてみよう)． さらに考察を進めて，すべての有理数解を求める手順を与えることもできるが，ここではあまり深入りしないことにしよう． なお，近似解を求めることも実用的にはきわめて重要ではあるが，この講義では話題にしない．

次に，a, b, c を 0 でない整数として，2変数の1次方程式

$$ax + by = c$$

を考えよう． 【数学A】で学んだように，この方程式が整数の組 (x, y) を解としてもつための条件は，c が a, b の最大公約数の倍数となることであった． また，実際に解を求めるには，ユークリッドの互除法が有効であった．

以上のように，ある方程式について，その整数解を問題にしたいとき，その方程式を**不定方程式**または**ディオファントス方程式**と呼ぶ． 解の範囲を自然数に狭めたり，逆に有理数に広げて考えたりすることもあり，その場合も不定方程式と呼ばれる．

数学，とくに代数学に属する分野，数論，代数幾何学，表現論などの研究を行うと，問題が不定方程式に帰着することが頻繁にある． それにともない，不定方程式の解法にも様々なアプローチがあるが，初等整数論はそのどれにも共通な基本的な手法になっている。

1.2　ピタゴラス方程式

古典的な不定方程式のひとつの例として**ピタゴラス方程式**を取り上げる．これは，直角 3 角形の 3 辺の関係を表す方程式

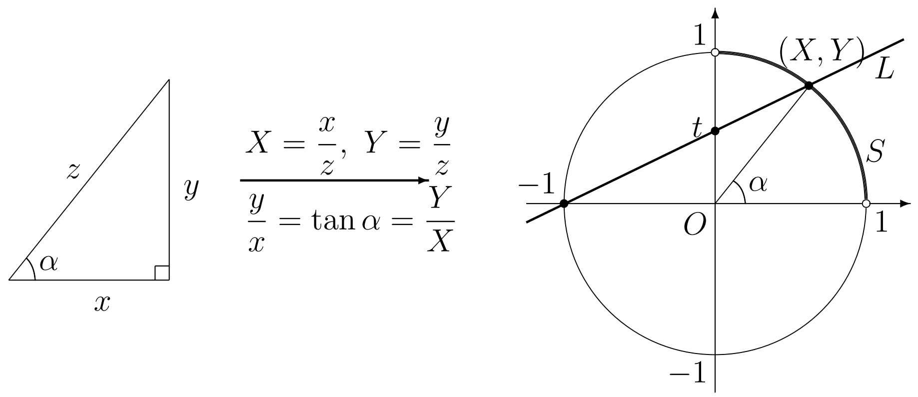
$$x^2 + y^2 = z^2$$

で，とくに辺の長さが自然数であるものに着目したものである．古代から $(x, y, z) = (3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$ などの解が知られており，一般の自然数解の求め方も解明されていたらしい（ネットで調べてみよ）．

ここでは，自然数とは一見関係なさそうな幾何学的な解法を紹介する．ピタゴラス方程式の自然数解を求めることは，

$$X^2 + Y^2 = 1$$

の正の有理数解を求めることと同等であることに注意する．実際，$x^2 + y^2 = z^2$ の自然数解 (x, y, z) から $X = x/z$, $Y = y/z$ とすれば $X^2 + Y^2 = 1$ の正の有理数解が得られ，逆に，$X^2 + Y^2 = 1$ の正の有理数解 (X, Y) を通分して $X = x/z$, $Y = y/z$ と表わせば $x^2 + y^2 = z^2$ の自然数解が得られるからである（くどい？）．このようにして，ピタゴラス方程式の自然数解は，原点を中心とする半径 1 の円周 S の上にある正の有理数を座標にもつ点（つまり第 1 象限にある点）と対応付けられることになる．いま，S 上のそのような点 (X, Y) と点 $(-1, 0)$ を通る直線 L を考えよう．このとき，下図を見れば，(X, Y) は L の Y-切片 t（$0 < t < 1$）と 1 対 1 に対応することがわかる．



直線 L の定義式 $Y = tX + t$ から

$$t = \frac{Y}{X + 1}$$

が得られるが，さらに $S\colon\ X^2 + Y^2 = 1$ と連立させれば，簡単な計算により

$$X = \frac{1 - t^2}{1 + t^2}, \qquad Y = \frac{2t}{1 + t^2}$$

が求まる．これらの式から，X, Y がともに有理数であることと t が有理数であることは同値であることがわかる．そこで，t に 0 と 1 の間の有理数を次々と代入すれば，

$t = \frac{1}{2}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \ldots$ の値から，対応する円周上の点

$$(X, Y) = \left(\frac{3}{5}, \frac{4}{5}\right), \quad \left(\frac{5}{13}, \frac{12}{13}\right), \quad \left(\frac{15}{17}, \frac{8}{17}\right), \quad \left(\frac{7}{25}, \frac{24}{25}\right), \ldots$$

を経由して，ピタゴラス方程式 $x^2 + y^2 = z^2$ の自然数解

$$(x, y, z) = (3, 4, 5), \quad (5, 12, 13), \quad (15, 8, 17), \quad (7, 24, 25), \ldots$$

が得られる． さらに重要なことは，この方法ですべての自然数解が得られることである．

1.3　フェルマーの最終定理

ピタゴラス方程式は 2 次式で表されているが，これを 3 次にするとどうなるか？ フェルマー（17 世紀の人）は，そのような方程式には自然数解がなく，さらに 4 次以上でも同様に自然数解がないと述べている． さらに，ある本の余白に,「その『驚くべき証明』を発見したがそれを記すにはこの余白は狭すぎる」と書き残した． 現在まで彼の証明は見つかっていない．

定理 1.1 (フェルマーの最終定理) 自然数 $n \geq 3$ に対して，方程式

$$x^n + y^n = z^n$$

は自然数解をもたない．

この定理は，長い間証明が知られていなかったので，かつては『フェルマー予想』とも呼ばれ，整数論における難問のひとつであった． フェルマー自身によって $n = 4$ の場合が証明され，$n = 3$ に対してはオイラーが証明を与えている（それぞれ，17, 18 世紀）．その後，ソフィー・ジェルマン，ディリクレ，クンマー等の貢献により，19 世紀中に 100 までのすべての n に対して正しいことが確かめられたが，20 世紀になって整数論や代数幾何学の理論が少しずつ整えられた結果，1994 年ワイルズによって完全な証明が与えられた． その証明は数多くの高度な理論を駆使して構成され，大胆な発想に満ちているが，その概略の一部だけでも紹介するにはこの余白は狭すぎる（なんちゃって）．

1.4　有名な問題

一般に数学の問題は難しい概念を用いて語られ，専門に学んだ人でなければ問題を理解することすら困難であることが多い． しかし，整数論の問題には初等的に表現されるものもあり，それらの多くは中高生でも（小学生でも？）理解できる． ただし，問題が初等的に表わされるからといって，必ずしも初等的に解けるとはいえず，未解決のまま残る

ことも往々にしてある． 前述の『フェルマーの最終定理（フェルマー予想）』も 25 年前まではそんな類の問題であった． 以下，素数に関する有名な予想について述べよう．

● 素数が無限個存在することは古代から知られているが，次の定理は，初項と公比が互いに素な数列上にも素数が無限に現れることを示している．

定理 1.2 (ディリクレ) 互いに素な整数 a, b（ただし $a > 0$）に対して $an+b$ $(n \in \boldsymbol{N})$ の形の素数が無限個存在する．

すなわち，係数が互いに素な 1 次式に自然数を代入していけば，素数が無数に現れる．

それでは，2 次以上の場合はどうか？ 2 次以上の整数係数の多項式（最高次係数は正）$f(x)$ に自然数を順々に代入していくと，$f(1), f(2), f(3), \cdots$ の中に素数が無限に現れるだろうか？ 現在までにそのような多項式 $f(x)$ はひとつも確認されていない（ひとつも！だぜっ）． もっとも簡単なケースとして次の予想がある．

予想 1.3 n^2+1 $(n \in \boldsymbol{N})$ の形の素数が無数に存在するであろう．

● $(3,5), (5,7), (11,13), (17,19)$ のように「差が 2 である素数のペア」も無数にありそうである． このようなペアを**双子素数**という． 計算を続けていくといくらでも大きなペアが見つかる，たとえば $(20200109, 20200111)$ など（Maple を使ってもっと探してみよ）．

予想 1.4 (双子素数予想) 双子素数は無限組存在するであろう．

双子素数は「差が 2 である素数のペア」であるが，2013 年,「差が 7 千万以下である素数のペア」が無数にあることが Y. Zhang によって証明された． “2 と 7 千万” では雲泥の差があるようだが，この証明以前には “2 と無限大” であったのだから，画期的な結果と言って良いであろう． その後すぐに改良が進み，7 千万が 246 に置き換えられることがわかった． いずれ，近いうちに 246 が 2 に改良され「双子素数予想」は解決されるのだろうか，それとも，新たな本質的な困難に突き当たって未解決のままになるのだろうか……．

● その数より小さい約数の和がその数になるとき**完全数**という． たとえば，28 はその約数 $1, 2, 4, 7, 14$ の和と等しいので完全数である． 2^n-1 が素数のとき $2^{n-1}(2^n-1)$ が完全数となることは古代から知られていた． さらにオイラーによって，偶数の完全数は必ずこのように表されることも証明されている (18 世紀).

予想 1.5 偶数の完全数は無限に存在するであろう．

この予想は，2^n-1 の形の素数が無数にあるだろう ということと同じである． このような素数は**メルセンヌ素数**と呼ばれ，巨大な素数の例として興味深い． 現在 (2020 年 3 月) までに 51 個のメルセンヌ素数が見つかっていて，最大のものは $2^{82589933}-1$（10 進表記で 24862048 桁）である． これは，明示的に知られている素数全体の中でも最大のものとなっている． なお，奇数の完全数は一つも発見されていない．

予想 1.6 奇数の完全数は存在しないであろう．