

ピタゴラス数

正の整数で $a^2 + b^2 = c^2$ を満たすとき、これをピタゴラス数という。たとえば、 $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$ がある。 $x^2 + y^2 = 1$ は円を表すから、ピタゴラス数は、円周上の有理数の組 $\left(\frac{a}{c}, \frac{b}{c}\right)$ が解となります。ほかにどんな数があるだろうか？

答え； $(8, 15, 17)$, $(9, 40, 41)$ などがあります。解の組は $a = u^2 - v^2$, $b = 2uv$, $c = u^2 + v^2$ として、 u, v に数を入れて求められます。なぜなら、等式 $(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$ であるから。

表計算ソフトで、この計算をしてみましょう。この例では、 (x, y) に対して、 $\sqrt{x^2 + y^2}$ が整数となるかどうかを判定し、もし整数であれば、1 を出力し、そうでなければ 0 としています。表計算での命令文は

`=if(sqrt(x^2+y^2)-int(sqrt(x^2+y^2))=0, 1, 0)`

としています。`sqrt` は平方根、`int` は値の整数化「ガウス記号」を表します。また各セルにこの命令文を代入するのはたいへんですから、コピーとペーストを行えば簡単です。そのためには2つの値 (x, y) を複合参照します。はじめのセル「c5」をアクティブにして、 x には\$B5, y にはc\$5 とします。この\$マークが片方にしかないことに注意してください（これが複合参照）。

数論における合同式 (modular arithmetic, congruence equation) は、 $A \equiv B \pmod{M}$ が成り立つとは、差 $A - B$ が M の倍数となるときと定めます。正確な等式との比較はできませんが、等式を構成するために、平方剰余の相互法則という整数の間での等式を構成する道具となります。

どの数が2つの平方数の和になるか？

定理：素数に関する2平方和定理 p を素数とすると、 p が2つの平方数の和で表せるのは

$$p \equiv 1 \pmod{4}$$

の場合のみである。

平方数の和となる素数	2,5,13,17,29,37,41,53,61,73,89,97,101,109,113,137,149,157
平方数の和とならない素数	3,7,11,19,23,31,43,47,59,67,71,79,83,103,107,127,131,139,151

この定理は2つの命題： p が2つの平方数の和であるならば、条件が成り立つことの証明は易しそうですね。素数 $p = a^2 + b^2$, $a = 2n + 1$, $b = 2m$ と仮定できます。これから $p = (2n + 1)^2 + (2m)^2 = 4n^2 + 4n + 1 + 4m^2 \equiv 1$ となり、証明できました。逆の証明はフェルマーの無限降下法という手続きが知られています。ここでは省略します。

定理：フェルマーの小定理 p を素数、 a を p で割り切れない自然数とすると、

$$a^{p-1} \equiv 1 \pmod{p}$$

たとえば、 $\frac{12345}{7}$ の計算では 商が1763、余りが4、つまり $12345 = 7 \times 1763 + 4$ 。フェルマーの小定理から、 $12345^6 \equiv 4^6 = 64^2 \equiv 1^2 = 1 \pmod{7}$ したがって 12345^6 を7で割った余りは1となる。

フェルマーの最終定理（大定理）とは、 $x^n + y^n = z^n$, $n = 3, 4, 5, \dots$ を満たす整数解は存在しない。いづれも17世紀の数学者フェルマー自身は証明を残してはいないが、最終定理はその後、1995年 Wiles が350年後に証明した。

平方数と三角数、自然数の和

平方数 n^2 は一辺の長さを n とする正方形の形に並べたものからきています。また三角数は三角形の形に並べたものからきています。三角数は $1+2=3, 1+2+3=6, 1+2+3+4=10$ ですから、 $3, 6, 10, \dots$ を指します。平方数は $1, 4, 9, 16, \dots$ です。

ここでは自然数の和を考えましょう。 $1+2+3+\dots+10=55$ 、また 1 から 24 まで加えると、 300 です。一般に $1+2+3+\dots+n=\frac{n(n+1)}{2}$ 。この式を求めるにはどう考えればよいだろうか。三角形を 2 つ考えると、対称形をもちいて計算できる。もし 2 乗和 $1^2+2^2+3^2+\dots+n^2$ では、どうなるでしょうか？この代わりに $1\cdot 2+2\cdot 3+3\cdot 4+4\cdot 5=40, 1\cdot 2+2\cdot 3+\dots+5\cdot 6=70$ となりますから、 $40=\frac{120}{3}=\frac{4\cdot 5\cdot 6}{3}$, $70=\frac{210}{3}=\frac{5\cdot 6\cdot 7}{3}$ という一般化を考えます。

答え； 2 乗和も図形的に求めるには、一つ三角形を回して作られる 3 つの三角形の総和を考える。 2 乗和の一般式は $1^2+2^2+3^2+\dots+n^2=\frac{n(n+1)(2n+1)}{6}$ となることを確かめよ。 2 項ずつの和は $1\cdot 2+2\cdot 3+n\cdot(n+1)=\frac{n(n+1)(n+2)}{3}$ となる。積分の公式 $\int x^2 dx = \frac{x^3}{3}$ と比べると、何か共通な点が感じられますね。

二項係数とパスカル三角形

2 項の和をベキ乗する計算式 $(a+b)^n$ を考えます。この展開に表れる係数は整数であり、記号では

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{k}a^{n-k}b^k + \dots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

2 項係数は $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ と定めます。ここで階乗 (factorial)

$$k! = \overbrace{k \cdot (k-1) \cdot (k-2) \cdots 3 \cdot 2 \cdot 1}^k$$

です。ただし $k \geq 0$ の整数で $0! = 1$ 。いままでの組合せ数 ${}_nC_k$ と一致しています。カッコをもちいた意味は、この組合せ数を負の数に拡張できるからです。

パスカル三角形もお馴染みの公式で、逐次的な上段との和を繰り返して得られます。

$$\begin{array}{rcccccc} (a+b)^4 & = & a^4 & +4a^3b & +6a^2b^2 & +4ab^3 & +b^4 \\ \times(a+b) & = & & a^4b & +4a^3b^2 & +6a^2b^3 & +4ab^4 & +b^5 \\ \hline & & a^5 & +4a^4b & +6a^3b^2 & +4a^2b^3 & +ab^4 & \\ \hline (a+b)^5 & = & a^5 & +5a^4b & +10a^3b^2 & +10a^2b^3 & +5ab^4 & +b^5 \end{array}$$

2 項係数の関係式：

$$(i) \binom{n}{k} = \binom{n}{n-k} \quad (ii) \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

$(a+b)^2 = a^2 + 2ab + b^2$ となる関係式はよく知られています。新たに定義として、 $a^{[1]} = a$, 2 項の増加積 $a^{[2]} = a(a+1)$, 3 項の増加積 $a^{[3]} = a(a+1)(a+2)$ などおくと、 $(a+b)^{[2]} = a^{[2]} + 2a^{[1]}b^{[1]} + b^{[2]}$ が成り立ちます。確かめてみましょう。また $a_{(1)} = a$, 2 項の減少積 $a_{(2)} = a(a-1)$, 3 項の減少積 $a_{(3)} = a(a+1)(a+2)$ を定義する場合、 $(a+b)_{(3)}$ と通常の $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$ と比較してみましょう。

またこの関係式を図に表して、把握理解できますので、講義時に説明します。