はじめに

本稿では, 原始ピタゴラス数が無数にあることの簡単な証明法 (第 1 節) と, すべての原始ピタゴラス数の決定 (第 2 節) について解説する. また, その応用として, フェルマーの最終定理の $n=4$ の場合の証明を与える (第 3 節). 大学初年級の学生が読むことを想定して書いたが, 難しい部分があるかもしれない.

1 原始ピタゴラス数

定義 1. ふたつ以上の整数 $a_1, a_2, \ldots, a_n$ の最大公約数を $\gcd(a_1, a_2, \ldots, a_n)$ と表す. $\gcd(a_1, a_2, \ldots, a_n) = 1$ のとき, 整数 $a_1, a_2, \ldots, a_n$ は互いに素であるという. また, 整数 a が整数 b を割り切るとき, $a|b$ と表す.

例 2. (1) $\gcd(8, 12, 20) = 4$　(2) $3, 4, 5$ は互いに素であるが, $6, 8, 10$ は互いに素ではない.　(3) $7|63$

定義 3. 正の整数の三つ組 (a, b, c) で $a^2+b^2 = c^2$ を満たすものを**ピタゴラスの三つ組** (Pythagorean Triple) あるいは単に**ピタゴラス数**という. 特に $\gcd(a, b, c) = 1$ (a, b, c が互いに素) のとき, **原始的なピタゴラスの三つ組**あるいは**原始ピタゴラス数**という.

4. 原始ピタゴラス数の簡単な見つけ方について説明する. a を 3 以上の奇数とすれば, a^2 も奇数なので,

$$a^2 = c + b, \quad c - b = 1$$

となる正の整数 b, c を見つけることができる. このとき, (a, b, c) はピタゴラス数である. なぜなら, $a^2 = (c + b) \cdot 1 = (c + b)(c - b) = c^2 - b^2$ より $a^2 + b^2 = c^2$ となるからである. 例えば,

$$\begin{aligned} 3^2 &= 9 = 5 + 4 = (5 + 4)(5 - 4) = 5^2 - 4^2, \\ 5^2 &= 25 = 13 + 12 = (13 + 12)(13 - 12) = 13^2 - 12^2, \\ 9^2 &= 81 = 41 + 40 = (41 + 40)(41 - 40) = 41^2 - 40^2 \end{aligned}$$

など (実際に例をいくつか作ってみよ). 最初のふた組 $(3, 4, 5)$, $(5, 12, 13)$ は有名で広く知られている.

このようにして見つけたピタゴラス数はすべて原始的である. 奇数 a は無数にあるので, 原始ピタゴラス数は無数に存在する. このことの証明を以下にキチンと示す. ふたつ示すが本質的にはどちらも同じである.

定理 5. 原始ピタゴラス数は無数に存在する.

証明その 1. a を 3 以上の任意の奇数とする. 奇数の 2 乗は奇数なので, $a^2 = 2n + 1$ とおくことができる (n は 4 以上の整数). このとき, $b = n$, $c = n + 1$ とすれば,

$$c^2 - b^2 = (c + b)(c - b) = (2n + 1) \cdot 1 = 2n + 1 = a^2$$

となるので

$$a^2 + b^2 = c^2$$

が成り立つ. また, b, c は隣り合う整数だから, $\gcd(a, b, c) = 1$ は明らかである. よって, (a, b, c) は原始ピタゴラス数である. 3 以上の奇数 a は無数にあるため, このような組も無数に存在する. □

証明その 2. a を 3 以上の任意の奇数とする. $a = 2m + 1$ (m は正の整数) とおくと, $a^2 = 4m^2 + 4m + 1$. このとき, $b = 2m^2 + 2m$, $c = 2m^2 + 2m + 1$ とすれば,

$$c^2 - b^2 = (c + b)(c - b) = (4m^2 + 4m + 1) \cdot 1 = 4m^2 + 4m + 1 = a^2$$

となるので

$$a^2 + b^2 = c^2$$

が成り立つ. また, b, c は隣り合う整数だから, $\gcd(a, b, c) = 1$ は明らかである. よって,

$$(a, b, c) = (2m + 1,\ 2m^2 + 2m,\ 2m^2 + 2m + 1) \tag{1}$$

は原始ピタゴラス数である. 正の整数 m は無数にあるため, このような組も無数に存在する. □

補注 6. 上の証明その 2 より, 式 (1) の形をした原始ピタゴラス数が無数にあることがわかった. しかし, すべての原始ピタゴラス数がこの形をしていると言っているわけではないので, 注意して欲しい.

2 すべての原始ピタゴラス数の決定

先に結論を述べ (定理 7), その後に例と証明を与える. 証明では整数の性質や三角比の性質がたくさん使われる. 例を量産することや証明の行間を埋めることは読者の練習とする.

定理 7. m, n を次の 3 条件を満たす整数とする. (1) $m > n > 0$, (2) $\gcd(m, n) = 1$, (3) $m - n$ は奇数. このとき,

$$(a, b, c) = (m^2 - n^2,\ 2mn,\ m^2 + n^2) \tag{2}$$

は原始ピタゴラス数である. 逆に, すべての原始ピタゴラス数は上の形で表すことができる.

補注 8. $m - n$ が奇数なら, $m + n = (m - n) + 2n$ も奇数である (奇数+偶数=奇数). よって, $a = m^2 - n^2 = (m + n)(m - n)$ は奇数である. これより, $c = m^2 + n^2 = (m^2 - n^2) + 2n^2$ も奇数である.

例 9. 証明の前に例を見る. $(m, n) = (2, 1)$ とすれば,

$$(a, b, c) = (2^2 - 1^2,\ 2 \cdot 2 \cdot 1,\ 2^2 + 1^2) = (3, 4, 5)$$

となる. これは前節で挙げた例と一致している. ところが, $(m, n) = (4, 1)$ とすれば,

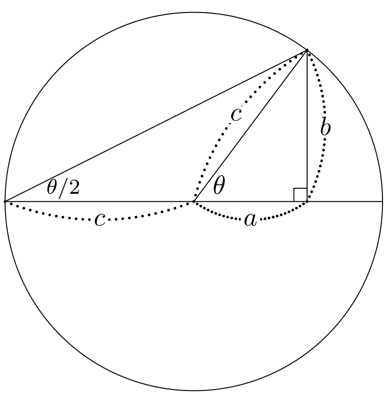
$$(a, b, c) = (4^2 - 1^2,\ 2 \cdot 4 \cdot 1,\ 4^2 + 1^2) = (15, 8, 17)$$

となる. これは前節の見つけ方では決して現れないものである (そのような具体例を他にも見つけよ).

定理 7 前半の証明. 式 (2) の (a, b, c) に対し $a^2 + b^2 = c^2$ が成り立つことは容易である (計算して確かめよ). 次に $\gcd(a, b, c) = 1$ を示すには $\gcd(a, b) = 1$ がわかれば十分である. そのために, $a = m^2 - n^2$ と $b = 2mn$ が共通の素因子を持たないことを示す.

p を $b = 2mn$ の素因子とする. 素数の性質より, $p = 2$ または $p|m$ または $p|n$ である ($p|m$ は「p は m を割り切る」の意味). 補注 8 より $a = m^2 - n^2$ は奇数なので, $p = 2$ は a の素因子にはなり得ない. 次に $p|m$ とする. $\gcd(m, n) = 1$ より $m + n$, $m - n$ はいずれも m と互いに素になるので, p は $a = (m + n)(m - n)$ の素因子にはなり得ない. $p|n$ の場合も同様である. □

定理 7 後半の証明. (a, b, c) を原始ピタゴラス数とすると, 3 辺の長さが a, b, c の直角三角形が存在する. そこで, 下図を考える. $0 < \theta < \dfrac{\pi}{2}$ である.



三角比の定義より

$$\tan\theta = \frac{b}{a}, \quad \cos\theta = \frac{a}{c}, \quad \sin\theta = \frac{b}{c} \tag{3}$$

である．次に, $t = \tan\frac{\theta}{2} = \frac{b}{a+c}$ とおく．これは $0 < t < 1$ なる有理数である．上の三角比を t で表すことを考える．三角比の公式

$$\tan\theta = \frac{2\tan\frac{\theta}{2}}{1-\tan^2\frac{\theta}{2}}, \quad \cos\theta = \sqrt{\frac{1}{1+\tan^2\theta}}, \quad \sin\theta = \tan\theta\cos\theta$$

を用いて計算すると,

$$\tan\theta = \frac{2t}{1-t^2}, \quad \cos\theta = \frac{1-t^2}{1+t^2}, \quad \sin\theta = \frac{2t}{1+t^2} \tag{4}$$

を得る (実際に計算して確かめよ)．よって, (3), (4) より

$$\frac{b}{a} = \frac{2t}{1-t^2}, \quad \frac{a}{c} = \frac{1-t^2}{1+t^2}, \quad \frac{b}{c} = \frac{2t}{1+t^2}$$

となり, これは $a : b : c = (1-t^2) : 2t : (1+t^2)$ を意味するから,

$$a = k\cdot(1-t^2), \quad b = k\cdot 2t, \quad c = k\cdot(1+t^2) \tag{5}$$

となる有理数 k が存在する．ここで, $t = \frac{n}{m}$ ($m > n > 0$, $\gcd(m,n) = 1$) とおけば, (5) は

$$a = \frac{k}{m^2}\cdot(m^2-n^2), \quad b = \frac{k}{m^2}\cdot 2mn, \quad c = \frac{k}{m^2}\cdot(m^2+n^2)$$

となる．このとき, 仮定 $\gcd(a,b,c) = 1$ より $\frac{k}{m^2} = 1$ および「$m-n$ は奇数」が従い,

$$a = m^2-n^2, \quad b = 2mn, \quad c = m^2+n^2$$

となる ($m-n$ が偶数なら a, b, c すべてが偶数になってしまうことを確認せよ). □

3 フェルマーの最終定理 ($n = 4$ の場合) の証明

原始ピタゴラス数の理論 (定理 7) を応用して, 次の定理の証明を与えよう．

定理 10 (フェルマー)**.** $X^4 + Y^4 = Z^4$ を満たす正の整数の組 (X, Y, Z) は存在しない．

証明. 背理法による．正の整数の組 (X, Y, Z) で

$$X^4 + Y^4 = Z^4 \tag{6}$$

を満たすものが存在するとしよう．もし $\gcd(X, Y, Z) = g > 1$ なら, (6) の両辺を g^4 で割れば最大公約数が 1 となる正の整数の組が得られるので, 初めから $\gcd(X, Y, Z) = 1$ として良い．このとき, $\gcd(X^2, Y^2, Z^2) = 1$ で, (6) より

$$(X^2)^2 + (Y^2)^2 = (Z^2)^2$$

なので, (X^2, Y^2, Z^2) は原始ピタゴラス数である．したがって, 定理 7 より

$$X^2 = M^2 - N^2 \tag{7}$$

$$Y^2 = 2MN \tag{8}$$

$$Z^2 = M^2 + N^2 \tag{9}$$

と表せる．ただし, M, N は正の整数で, $M > N > 0$, $\gcd(M, N) = 1$, $M - N$ は奇数. (注意. (7) と (8) は X^2 が奇数で Y^2 が偶数の場合である．ふたつの偶奇が逆の場合はあらかじめ入れ替えておけば良い.)

さて, (7) と (9) に着目しよう．(この 2 式に再び定理 7 を適用することがこの証明の核心である.)

(7) より $X^2 + N^2 = M^2$. また, $\gcd(M, N) = 1$ より $\gcd(X, M, N) = 1$ である．よって, (X, N, M) は原始ピタゴラス数. X^2 が奇数なので X も奇数だから, 定理 7 より

$$X = a^2 - b^2 \tag{10}$$
$$N = 2ab \tag{11}$$
$$M = a^2 + b^2 \tag{12}$$

と表せる (N は偶数, M は奇数となることに注意). ただし, a, b は正の整数で, $a > b > 0$, $\gcd(a, b) = 1$, $a - b$ は奇数.

同様に, (9) より (M, N, Z) は原始ピタゴラス数. M が奇数で N が偶数だから, 定理 7 より

$$M = c^2 - d^2 \tag{13}$$
$$N = 2cd \tag{14}$$
$$Z = c^2 + d^2 \tag{15}$$

と表せる．ただし, c, d は正の整数で, $c > d > 0$, $\gcd(c, d) = 1$, $c - d$ は奇数.

これより, 矛盾を導き出す段階に入る.

(11)〜(14) より

$$M = a^2 + b^2 = c^2 - d^2 \tag{16}$$
$$N = 2ab = 2cd \tag{17}$$

となる．(16) と (17) の辺々を加えて因数分解すると

$$M + N = (a + b)^2 = (c - d)^2$$

となり, $a + b > 0$, $c - d > 0$ より $a + b = c - d$ を得る．ここで, (10) と (13) を見ると

$$X = a^2 - b^2 = (a + b)(a - b)$$
$$M = c^2 - d^2 = (c + d)(c - d)$$

なので, $a + b = c - d$ は X と M の共通因子になっている． ところが, $\gcd(X, M) = 1$ なので (もし $\gcd(X, M) > 1$ なら $N^2 = M^2 - X^2$ より $\gcd(X, M, N) = 1$ に矛盾する), $a + b = c - d = 1$ となる他ない. これは a, b が正の整数であることに矛盾する. □

考えられる課題

- 式 (1) を用いての原始ピタゴラス数のリストの作成 (表計算ソフトの利用)
- 定理 7 を用いての原始ピタゴラス数のリストの作成 (同上)
- 三角関数 (三角比) の取り扱いの復習
- 整数の基本性質の復習 (例えば, 奇数+偶数=奇数の証明など)
- 初等整数論の研究
- 定理 5 の別証明を考えてみる
- フェルマーの最終定理についての調査・研究
- 歴史研究

など.

参考文献等

本稿の作成にあたり以下のサイトを参考にしました.
http://izumi-math.jp/sanae/MathTopic/py_num/py_num.htm

また, 第 3 節追加の際に「代数の魅力」(木村・竹内・宮本・森田著, 数学書房) を参考にしました. 定理 10 の証明が少し異なります (本質は変わらないが矛盾の導出方法が少し異なる) ので, 興味がある方はこちらを参照してください.

更新履歴

2012/11/28 初稿
2012/11/29 第 2 稿
2013/01/25 第 3 稿
2013/06/07 第 4 稿 (第 3 節追加)