

基礎教育科目「数学再発見」概要

久木田英史

鍵語：基礎教育・数学教育・数学史・整数論・幾何学

「数学再発見（数と形の不思議）」は本学における学部改組（2019年度）に伴い、基礎教育科目の一つとして構想された。この科目は整数論や幾何学分野で、数学史上有名でありながら初等・中等教育では扱われない命題を素材に、計算や作図のような作業を通して、一見単純な数や図形に潜む美しい性質を自ら見出していく知的愉悅を受講者に経験してもらうことを、第一の目的とする。以下、その骨格となる内容を整理し、講義の概要として示す。

1 オイラー円とフォイエルバッハの定理

幾何学分野では、高校数学で学んだ三角形の五心（外心、重心、垂心、内心、傍心）の復習から出発して、これらの点の相互関係を探求し、古典的な平面幾何学の到達点の一つ、フォイエルバッハの定理の理解に至ることを目標とする。

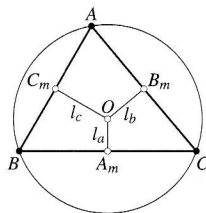
1.1 外心、重心、垂心の作図

以下、特に断らない限り、三角形 ABC において、辺 BC, CA, AB の中点をそれぞれ A_m, B_m, C_m とする。また、頂点 A, B, C から対辺に下ろした垂線の足をそれぞれ A_h, B_h, C_h とする。

定理 1.1.1 任意の三角形 ABC において、 A_m を通り BC と垂直な直線を l_a 、 B_m を通り CA と垂直な直線を l_b 、 C_m を通り AB と垂直な直線を l_c とすれば、 l_a, l_b, l_c は一点で交わる。

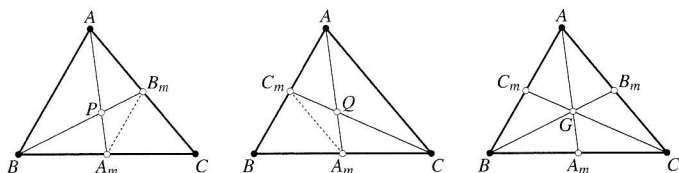
証明 線分 BC の垂直二等分線 l_a 上の任意の点は二点 B, C から等距離である。同じく、線分 CA の垂直二等分線 l_b 上の任意の点は二点 C, A から等距離である。ゆえに、 l_a と l_b の交点を O とすれば、 O は二点 A, B から等距離で、線分 AB の垂直二等分線 l_c の上にある。□

O は A, B, C から等距離なので、この三点を通る円の中心である。円 ABC を三角形 ABC の外接円、点 O を三角形 ABC の外心という。



定理 1.1.2 任意の三角形 ABC において、三直線 AA_m, BB_m, CC_m は一点で交わり、その交点は線分 AA_m, BB_m, CC_m をそれぞれ $2:1$ に内分する。

証明 AA_m と BB_m の交点を P とする。中点連結定理により、三角形 ABP と A_mB_mP は相似で、 $AB = 2A_mB_m$ なので、 $AP : A_mP = 2 : 1$ となる。同様に、 AA_m と CC_m の交点を Q とすれば $AQ : A_mQ = 2 : 1$ となり、 P と Q は一致する。 \square



定理 1.1.2 の交点を G として、三角形 ABG, BCG, CAG は三角形 ABC の面積を三等分するので、 G を三角形 ABC の重心という。

定理 1.1.3 任意の三角形 ABC において、三直線 AA_h, BB_h, CC_h は一点で交わる。

証明 三角形の各頂点を通り、その対辺に平行な三直線について、その交点を左図のように A', B', C' とする。

四角形 $ABCB', ACBC'$ はそれぞれ平行四辺形なので $AB' = BC$ かつ $AC' = BC$ 、よって A は線分 $B'C'$ の中点である。また、 $B'C'$ は BC と平行なので、 AA_h と垂直に交わる。従って、 AA_h は線分 $B'C'$ の垂直二等分線である。同様に、 BB_h, CC_h はそれぞれ線分 $C'A', A'B'$ の垂直二等分線なので、三角形 $A'B'C'$ において、定理 1.1.1 より、 AA_h, BB_h, CC_h は一点で交わる。 \square

定理 1.1.3 の交点を H として、 H を三角形 ABC の垂心という。

上の証明における A, B, C をそれぞれ A_m, B_m, C_m と読み替え、 A', B', C' をそれぞれ A, B, C と読み替えると、次の命題が得られる。

系 1.1.3.1 三角形 ABC の外心と三角形 $A_mB_mC_m$ の垂心は一致する。

1.2 外心、重心、垂心の位置関係

以下、特に断らない限り、三角形 ABC の外心、重心、垂心をそれぞれ O, G, H とする。三点の相互関係を調べるために、定理 1.1.3 を前節とは別の方法で証明する。

定理 1.1.3 の別証 AA_h と BB_h の交点を P とし、 O に関する C の対称点を C' とする。線分 CC' は三角形 ABC の外接円の直径なので、角 CAC' と CBC'

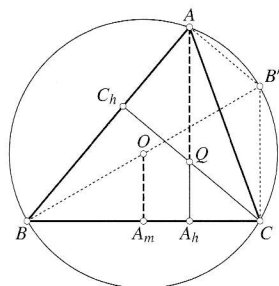
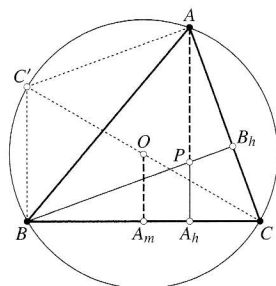
は共に直角である。よって AC' と BP は平行、また BC' と AP も平行で、四角形 $AC'BP$ は平行四辺形、ゆえに

$$BC' = AP$$

他方、 BC' は OA_m と平行なので、中点連結定理により

$$BC' = 2OA_m$$

以上により、 $AP = 2OA_m$ を得る。



他方、 AA_h と CC_h の交点を Q とし、 O に関する B の対称点を B' とすれば、上と同様に $AQ = 2OA_m$ 、従って P と Q は同一の点で、 H と一致する。□
この別証から、次の命題が導かれる。

定理 1.2.1 任意の三角形 ABC において、

$$AH : OA_m = 2 : 1 \quad (1.2.1)$$

が成り立つ。

定理 1.2.2 任意の三角形 ABC において、 O, G, H は同一直線上にあり、 G は線分 HO を $2 : 1$ に内分する。

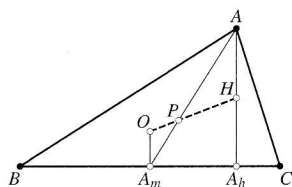
証明 HO と AA_m の交点を P とする。 OA_m と AA_h は平行なので、三角形 AHP と A_mOP は相似で、(1.2.1) により相似比は $2 : 1$ 、ゆえに

$$AP : A_mP = 2 : 1 \quad \text{かつ} \quad HP : OP = 2 : 1$$

となるが、第一式は定理 1.1.2 により P が G と一致していることを示しているので、第二式は

$$HG : OG = 2 : 1 \quad (1.2.2)$$

と書き換えられる。□

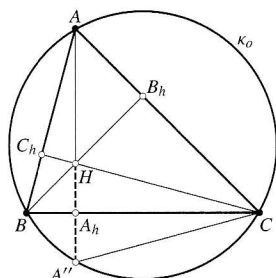
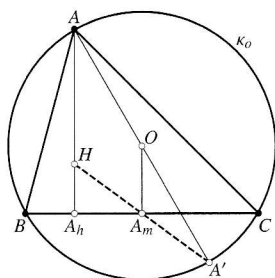


1.3 外心、重心、垂心とオイラー円

以下、特に断らない限り、三角形 ABC の外接円を κ_o とする。

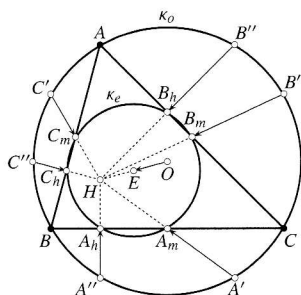
定理 1.3.1 任意の三角形 ABC について、以下が成り立つ。

- (1) A_m に関して H と対称な点は κ_o 上にある。
- (2) A_h に関して H と対称な点は κ_o 上にある。



証明 (1) O に関して A と対称な点を A' とすれば、 A' は明らかに κ_o 上にある。ここで三角形 AHA' と OA_mA' は相似で、相似比は $2:1$ なので、 A' は A_m に関して H と対称である。

(2) 角 AHC_h と CHA_h は等しいので、直角三角形 AHC_h と CHA_h は相似である。他方、直線 AA_h が κ_o と改めて交わる点を A'' とすれば、角 BAA'' と BCA'' は同一の弧に対する円周角として等しいので、直角三角形 AHC_h と $CA''A_h$ も相似である。ここで、三角形 CHA_h と $CA''A_h$ は辺 CA_h を共有するので合同、従って $HA_h = A''A_h$ となる。 \square



定理 1.3.2 任意の三角形 ABC において、 $A_m, A_h, B_m, B_h, C_m, C_h$ は同一円周上にある。

証明 点を表す文字の対称性を考慮すれば、定理 1.3.1 の A', A'' に加え、

- (3) B_m に関する H の対称点 B'
- (4) B_h に関する H の対称点 B''
- (5) C_m に関する H の対称点 C'
- (6) C_h に関する H の対称点 C''

はいずれも κ_o 上にある。いま、 H を中心とする変倍率 0.5 の相似変換を \mathcal{H}_h とすれば、以上の結果は、 $A_m, A_h, B_m, B_h, C_m, C_h$ の各点がそれぞれ、 κ_o 上の点 $A', A'', B', B'', C', C''$ の \mathcal{H}_h による像

であり、従って、 κ_o の \mathcal{H}_h による像 $\mathcal{H}_h(\kappa_o)$ の上にあることを示している。

ここで、 $\mathcal{H}_h(\kappa_o)$ は円と相似な図形、すなわち円で、その半径は元の円 κ_o の半径の 0.5 倍、中心は κ_o の中心 O の \mathcal{H}_h による像 $\mathcal{H}_h(O)$ 、すなわち線分 HO の中点である。 \square

定理 1.3.2 で述べられた、 $A_m, A_h, B_m, B_h, C_m, C_h$ を通る円を、三角形 ABC のオイラー円という。以下、特に断らない限り、オイラー円を κ_e 、その中心を E とする。

定理 1.3.3 任意の三角形 ABC において、

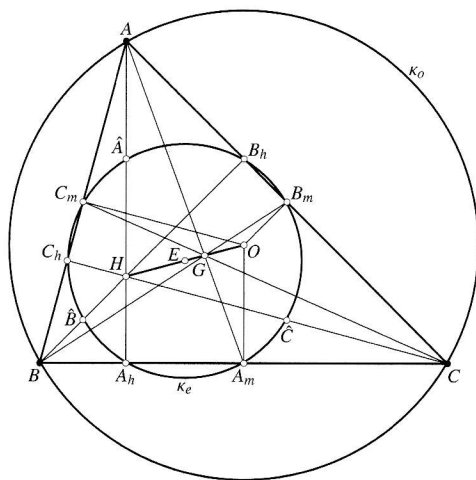
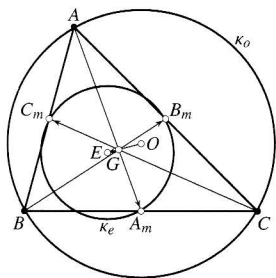
$$OG : GE : EH = 2 : 1 : 3 \quad (1.3.1)$$

が成り立つ。

証明 線分 AA_m, BB_m, CC_m に注目すれば、定理 1.1.2 により、 κ_e は中心 G 、変倍率 -0.5 の相似変換 \mathcal{H}_g による κ_o の像とも解釈され、従って、 G は線分 OE を $2:1$ に内分する。このことと、 E が線分 HO の中点であることを考慮すれば、結論を得る。 \square

再び中心 H の相似変換 \mathcal{H}_h に戻り、線分 AH, BH, CH の中点をそれぞれ $\hat{A}, \hat{B}, \hat{C}$ とすれば、これらはそれぞれ、 κ_o 上の点 A, B, C の \mathcal{H}_h による像なので、全て κ_e の上にある。

以上述べられた、三角形 ABC におけるオイラー円 κ_e の性質を、改めて整理する。

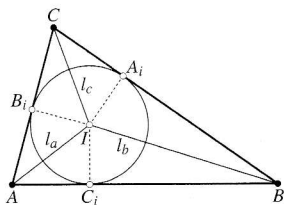


- (1) 各辺の中点 A_m, B_m, C_m を全て含む。
- (2) 各頂点から対辺に下ろした垂線の足 A_h, B_h, C_h を全て含む。
- (3) 垂心と各頂点を結ぶ線分の中点 $\hat{A}, \hat{B}, \hat{C}$ を全て含む。
- (4) 半径は外接円 κ_o の半径の 0.5 倍である。
- (5) 中心 E について、 $OG : GE : EH = 2 : 1 : 3$ 。

上述の (1) から (3) までの性質により、 κ_e を三角形 ABC の九点円ともいう。

1.4 内心、傍心の作図

定理 1.4.1 任意の三角形 ABC において、三つの頂点の内角の二等分線は一点で交わる。



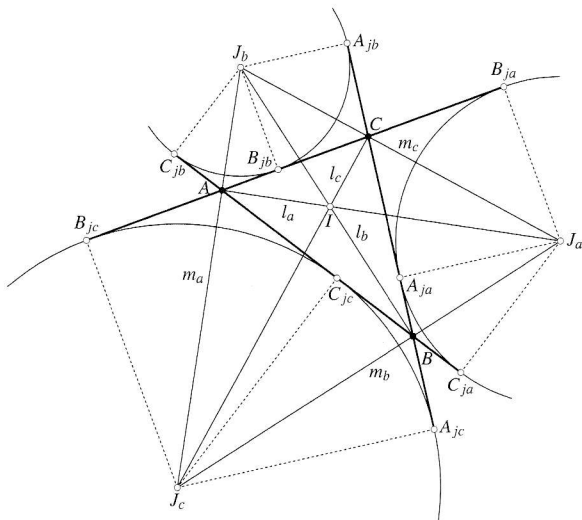
証明 頂点 A, B, C の内角の二等分線をそれぞれ l_a, l_b, l_c とする。 l_b 上の任意の点は二辺 BC, CA から等距離である。同じく、 l_c 上の任意の点は二辺 CA, AB から等距離である。ゆえに、 l_b と l_c の交点を I とすれば、 I は AB, CA から等距離で、 l_a の上にある。□

I から BC, CA, AB に下ろした垂線の足をそれぞれ A_i, B_i, C_i とすれば、

$$IA_i = IB_i = IC_i$$

なので、 I は三点 A_i, B_i, C_i を通る円の中心である。円 $A_iB_iC_i$ を三角形 ABC の内接円、点 I を三角形 ABC の内心という。

定理 1.4.2 任意の三角形 ABC において、任意の一つの頂点の内角の二等分線は、それ以外の二つの頂点の外角の二等分線と一点で交わる。



証明 定理 1.4.1 の証明における l_a, l_b, l_c に加え、頂点 A, B, C の外角の二等分線をそれぞれ m_a, m_b, m_c とする。 m_b 上の任意の点は二辺 BC, CA から等距離である。同じく、 m_c 上の任意の点は二辺 CA, AB から等距離である。ゆ

えに、 m_b と m_c の交点を J_a とすれば、 J_a は AB, CA から等距離で、 l_a の上にある。

m_c と m_a の交点 J_b が l_b 上にあること、 m_a と m_b の交点 J_c が l_c 上にあることも、同様に示される。□

J_a から BC, CA, AB に下ろした垂線の足をそれぞれ A_{ja}, B_{ja}, C_{ja} とすれば、

$$J_a A_{ja} = J_a B_{ja} = J_a C_{ja}$$

なので、 J_a は三点 A_{ja}, B_{ja}, C_{ja} を通る円の中心である。円 $A_{ja}B_{ja}C_{ja}$ を頂点 A に対する三角形 ABC の傍接円、点 J_a を頂点 A に対する三角形 ABC の傍心という。

同様に、 J_b を頂点 B に対する傍心、 J_c を頂点 C に対する傍心という。

定理 1.4.3 任意の三角形 ABC において、三個の傍心を頂点とする三角形 $J_a J_b J_c$ の垂心は、三角形 ABC の内心と一致する。

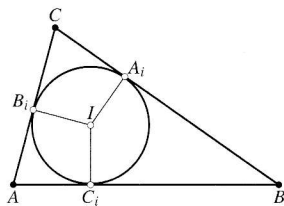
証明 定理 1.4.1 と定理 1.4.2 における l_a, l_b, l_c と m_a, m_b, m_c について、後者は三角形 $J_a J_b J_c$ の三辺であり、前者はこの三角形のそれぞれの頂点から対辺に下ろした垂線である。□

1.5 内接円、傍接円の性質

以下、特に断らない限り、三角形 ABC の内心を I 、内接円を κ_i とする。また、頂点 A, B, C に対する傍心をそれぞれ J_a, J_b, J_c とし、各傍心を中心とする傍接円をそれぞれ $\kappa_{ja}, \kappa_{jb}, \kappa_{jc}$ とする。内心や傍心から各辺に下ろした垂線の足は、定理 1.4.1 や定理 1.4.2 の図の通りとする。最後に、辺 BC, CA, AB の長さをそれぞれ a, b, c とし、 $s = (a + b + c)/2$ とおく。

定理 1.5.1 任意の三角形 ABC において、内心 I から三辺に下ろした垂線の足 A_i, B_i, C_i について、

$$\begin{aligned} AB_i &= AC_i = s - a \\ BC_i &= BA_i = s - b \\ CA_i &= CB_i = s - c \end{aligned} \quad (1.5.1)$$



が成り立つ。

証明 $AB_i = AC_i = x$, $BC_i = BA_i = y$, $CA_i = CB_i = z$ とおけば

$$BA_i + CA_i = BC, \quad CB_i + AB_i = CA, \quad AC_i + BC_i = AB$$

すなわち

$$y + z = a, \quad z + x = b, \quad x + y = c$$

この三式を辺々足せば $2(x+y+z) = a+b+c$ 、すなわち $x+y+z = s$ となり、

$$x = (x+y+z) - (y+z) = s - a$$

$$y = (x+y+z) - (z+x) = s - b$$

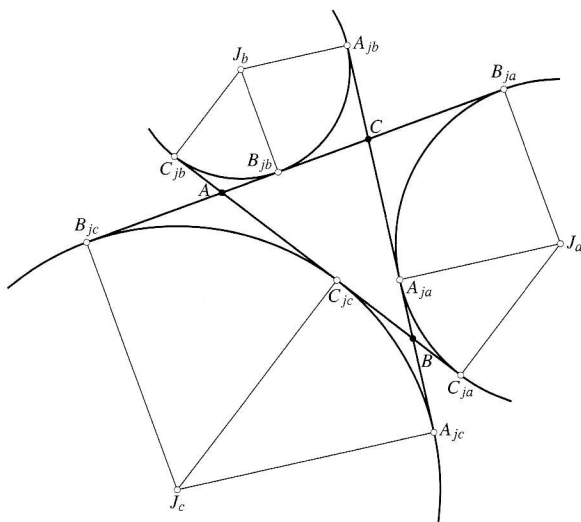
$$z = (x+y+z) - (x+y) = s - c$$

として結論を得る。 □

定理 1.5.2 任意の三角形 ABC において、傍心 J_a から辺 BC に下ろした垂線の足 A_{ja} 、傍心 J_b から辺 CA に下ろした垂線の足 B_{jb} 、傍心 J_c から辺 AB に下ろした垂線の足 C_{jc} について、

$$\begin{aligned} BA_{ja} &= s - c, & CA_{ja} &= s - b \\ CB_{jb} &= s - a, & AB_{jb} &= s - c \\ AC_{jc} &= s - b, & BC_{jc} &= s - a \end{aligned} \tag{1.5.2}$$

が成り立つ。



証明 最初の二式について、

$$\begin{aligned} AC_{ja} + AB_{ja} &= (AB + BC_{ja}) + (AC + CB_{ja}) \\ &= (AB + BA_{ja}) + (AC + CA_{ja}) \\ &= (BA_{ja} + CA_{ja}) + AB + AC \\ &= a + b + c = 2s \end{aligned}$$

すなわち $AC_{ja} = AB_{ja} = s$ なので、

$$BA_{ja} = BC_{ja} = AC_{ja} - AB = s - c$$

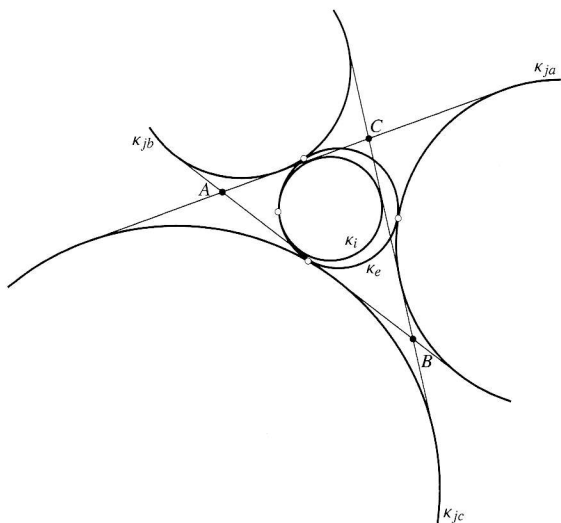
$$CA_{ja} = CB_{ja} = AB_{ja} - AC = s - b$$

として結論を得る。残りの四式も同様に求められる。

□

1.6 内接円、傍接円とオイラー円

定理 1.6.1 任意の三角形 ABC において、内接円 κ_i と三つの傍接円 $\kappa_{ja}, \kappa_{jb}, \kappa_{jc}$ は全て、オイラー円 κ_e に接する。

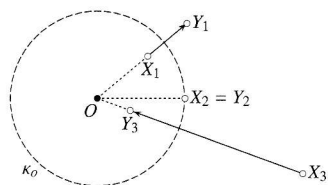


定理 1.6.1 は発見者 Karl Wilhelm Feuerbach (1800-1834) の名前に因んで、「フョエルバッハの定理」と呼ばれる。定理の内容の単純明快な美しさに比べ、証明は一般に困難であるが、ここでは「円に関する反転」という技法による鮮やかな証明を紹介する。

定義 κ_o を中心 O 、半径 r の円とする。
いま、 κ_o と同じ平面上の任意の点 X と、 O を起点とする半直線 OX 上の点 Y が

$$OX \cdot OY = r^2 \quad (1.6.1)$$

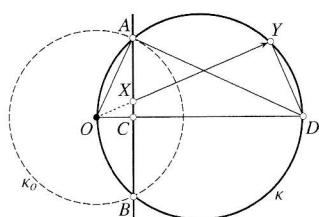
という条件を満たすとする。このとき、 X を Y に移す操作を、円 O に関する X の反転と



いう。また、 Y を反転による X の像という。 Y が X の像であるとき、 X は Y の像でもある。

「反転」という名称は、この操作により、 κ_o の内部の点が外部に、外部の点が内部に移されることに由来する。 κ_o の円周上の点は、反転により元の位置に留まる。任意の点は、反転の二度の操作により、元の位置に戻る。

以下、上記の κ_o に関する反転の、二つの例を取り上げる。例 1.6.1 では直線が円に移され、例 1.6.2 では円がそれ自体に移される。

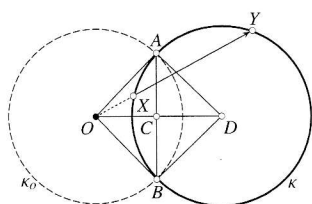


例 1.6.1 κ_o の中心 O を通る円 κ が、 κ_o と点 A, B で交わるとする。いま、直線 AB 上の任意の点 X に対し、 O を起点とする半直線 OX が、点 Y において再び κ と交わるとする。このとき Y は、 κ_o に関する反転による X の像である。

実際、三角形 OCX と OYD は相似なので $OC : OX = OY : OD$ 、よって $OX \cdot OY = OC \cdot OD$ である。また、三角形 OAC と ODA は相似な

ので $OA : OC = OD : OA$ 、よって $OC \cdot OD = OA^2 = r^2$ である。ゆえに $OX \cdot OY = r^2$ が成り立つ。

いま、 Y が κ 上で O に限りなく近づく、 X は直線 AB 上で、線分 AB の中点 C から限りなく遠ざかっていく。このことから、直線 AB の上下双方向の無限遠の距離に、 AB と平行な別の直線(O における κ の接線など)との交点として、ある一つの点 $(AB)_\infty$ (AB 上の無限遠点)が存在し、この点が反転により、反転の中心 O に移されると解釈する。



例 1.6.2 κ_o が円 κ と点 A, B で交わり、交点における二つの円の接線が互いに垂直に交わるとする。いま、 κ 上の任意の点 X に対し、 O を起点とする半直線 OX が、点 Y において再び κ と交わるとする。このとき Y は、 κ_o に関する反転による X の像である。

実際、円 κ に対する点 O の方べきを考えれば、 $OX \cdot OY = OA^2 = r^2$ となる。

以上の予備考察を踏まえ、ここから実際に、

フォイエルバッハの定理を証明する。

証明 内接円 κ_i と傍接円の一つ κ_{ja} について考察する。 κ_{ja}, J_a, A_{ja} はそれぞれ、 κ_j, J, A_j と略記する。

$b = c$ の場合、 κ_i と κ_j が辺 BC の中点 A_m において κ_e と接するのは明らかなので、 $b > c$ と仮定する。

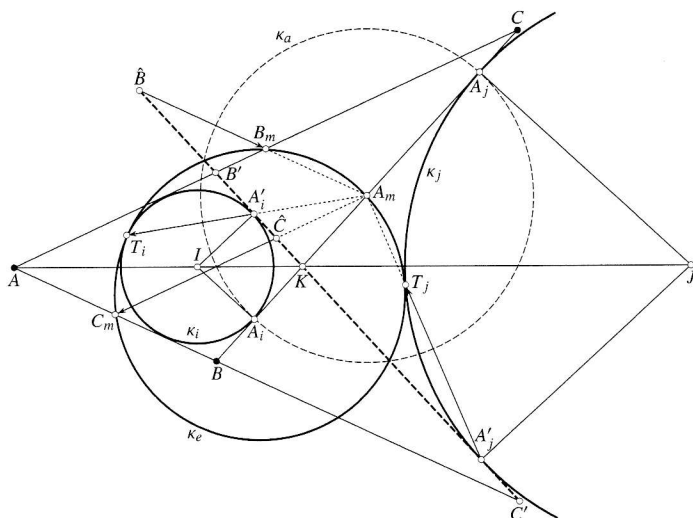
頂点 A の内角の二等分線 AIJ に関して B, C と対称な点を、それぞれ B', C' とする。三直線 $AIJ, BC, B'C'$ は一点で交わるので、この交点を K とする。

I, J から $B'C'$ に下ろした垂線の足を A'_i, A'_j とすれば、 $B'C'$ は明らかに、 A'_i において κ_i に接し、 A'_j において κ_j に接する。

線分 A_iA_j を直径とする円を κ_a とする。定理 1.5.1 と定理 1.5.2 により $BA_i = CA_j = s - b$ なので、 κ の半径は

$$\frac{BC - BA_i - CA_j}{2} = \frac{a - 2(s - b)}{2} = \frac{b - c}{2} \quad (1.6.2)$$

また、 A_i と A_j は A_m に関して対称なので、 κ_a の中心は A_m である。



いま、円 κ_a に関する反転を I とする。以下、 I により

[A] 直線 $B'C'$ はオイラー円 κ_e に移され、

[B] 内接円 κ_i は κ_i 自体に、傍接円 κ_j は κ_j 自体に移されることを、順次確かめていく。

[A] 直線 $B'C'$ とオイラー円 κ_e について、 $B'C'$ と A_mB_m との交点を \hat{B} とし、 A_mC_m との交点を \hat{C} とする。三角形 $A_m\hat{B}K$ と $BC'K$ 、 $A_m\hat{C}K$ と $CB'K$ はそれぞれ相似なので

$$A_m\hat{B} : A_mK = BC' : BK, \quad A_m\hat{C} : A_mK = CB' : CK$$

すなわち

$$A_m\hat{B} = \frac{BC'}{BK} \cdot A_mK, \quad A_m\hat{C} = \frac{CB'}{CK} \cdot A_mK$$

ここで

$$BC' = CB' = AC - AB = b - c$$

点 K は頂点 A の内角の二等分線上にあり、辺 BC を $c:b$ に内分するので

$$BK = \frac{ac}{b+c}, \quad CK = \frac{ab}{b+c}$$

このとき

$$A_mBK = A_mB - BK = \frac{a}{2} - \frac{ac}{b+c} = \frac{a(b-c)}{2(b+c)}$$

なので

$$A_m\hat{B} = (b-c) \cdot \frac{b+c}{ac} \cdot \frac{a(b-c)}{2(b+c)} = \frac{(b-c)^2}{2c}$$

$$A_m\hat{C} = (b-c) \cdot \frac{b+c}{ab} \cdot \frac{a(b-c)}{2(b+c)} = \frac{(b-c)^2}{2b}$$

よって

$$\begin{aligned} A_mB_m \cdot A_m\hat{B} &= \frac{c}{2} \cdot \frac{(b-c)^2}{2c} = \left(\frac{b-c}{2}\right)^2 \\ A_mC_m \cdot A_m\hat{C} &= \frac{b}{2} \cdot \frac{(b-c)^2}{2b} = \left(\frac{b-c}{2}\right)^2 \end{aligned} \tag{1.6.3}$$

を得る。(1.6.3) は (1.6.1) と (1.6.2) によれば、 I により、直線 $B'C'$ 上の点 \hat{B} と \hat{C} がそれぞれ、オイラー円 κ_e の円周上の点 B_m と C_m に移されることを示している。更に、 κ_e は反転の基準円 κ_a の中心 A_m を通るが、例 1.6.1 によれば、このとき A_m は、直線 $B'C'$ 上の無限遠点 $(B'C')_\infty$ の I による像なのだった。こうして I により、 $B'C'$ を定める三点 $(B'C')_\infty, \hat{B}, \hat{C}$ がそれぞれ、 κ_e を定める三点 A_m, B_m, C_m に対応付けられるので、 $B'C'$ 上の任意の点は I により、 κ_e 上のいずれかの点に移される。

[B] 内接円 κ_i と傍接円 κ_j について。点 A_i において、 κ_i の接線 A_iA_j と κ_a の接線 A_iI は垂直に交わる。また、点 A_j において、 κ_j の接線 A_jA_i と κ_a の接線 A_jI は垂直に交わる。よって例 1.6.2 で述べたように、 I により、 κ_i 上の任意の点は κ_i 自体の上のいずれかの点に、 κ_j 上の任意の点は κ_j 自体の上のいずれかの点に移される。

[A] と [B] から、次の結論が導かれる。すなわち I により、 $B'C'$ と κ_i の共通部分は κ_e と κ_i の共通部分に移され、 $B'C'$ と κ_j の共通部分は κ_e と κ_j の共通部分に移される。いま、 $B'C'$ と κ_i は A'_i で接するので、 κ_e と κ_i は I による A'_i の像 T_i で接する。また、 $B'C'$ と κ_j は A'_j で接するので、 κ_e と κ_j は I による A'_j の像 T_j で接する。□

2 ピタゴラス数からフェルマーの定理へ

整数論分野では、こちらも高校数学で触れられるピタゴラス数（三平方の定理を満たす三個の自然数の組）を網羅的に見出す公式を探求し、その自然な展開として、解決に三世紀半以上もの歳月を要した、数学史上最高難度の問題「フェルマーの定理」のあらましを知ること目標とする。

2.1 既約ピタゴラス数

三平方の定理（ピタゴラスの定理）によれば、任意の直角三角形において、 a と b を直角を挟む二辺の長さ、 c を斜辺の長さとして、

$$a^2 + b^2 = c^2 \quad (2.1.1)$$

が成り立つ。(2.1.1) を満たす三個の自然数の組 (a, b, c) をピタゴラス数という。

ここで最初に探求する「ピタゴラス数は無数に存在するか」という問いに対する答えは、ある意味自明である。例えば右図のように、直角を挟む二辺の長さが3と4の直角三角形において、斜辺の長さは5で、

$$3^2 + 4^2 = 5^2 \quad (2.1.2)$$

すなわち $9 + 16 = 25$ が成り立つ。このピタゴラス数 $(3, 4, 5)$ について、その各数を整数倍した任意の

$$(3k, 4k, 5k) \quad (k > 1 \text{ は整数})$$

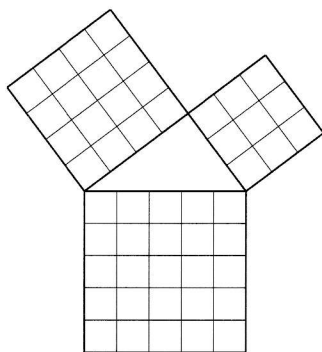
を考えると、

$$(3k)^2 + (4k)^2 = (5k)^2 \quad \text{すなわち} \quad (3^2 + 4^2)k^2 = 5^2k^2$$

は両辺を $k^2 \neq 0$ で割ることで、(2.1.2) に帰着する。このような興味を欠く例を避けるために、以下、考察の対象は、 a, b, c が互いに素である場合、すなわち、これら三個の数が既約で、その最大公約数が1である場合に限ることにする。

定理 2.1.1 (a, b, c) が既約ピタゴラス数として (2.1.1) を満たすとき、左辺の a と b のうち一方は偶数であり、他方は奇数である。また、右辺の c は奇数である。

証明 a と b を共に偶数と仮定すれば、(2.1.1) の左辺は偶数なので c^2 が偶数、従って c も偶数となるが、これは a, b, c が既約という前提に反する。



a と b を共に奇数と仮定すれば、適当な整数 x と y により $a = 2x+1$, $b = 2y+1$ と表される。このとき

$$a^2 + b^2 = (2x+1)^2 + (2y+1)^2 = 2(2x^2 + 2y^2 + 2x + 2y + 1)$$

なので、 c は偶数である。適当な整数 z により $c = 2z$ と表すと

$$(2x+1)^2 + (2y+1)^2 = (2z)^2$$

両辺を 2 で割って整理すると

$$2(x^2 + y^2 + x + y) + 1 = 2z^2$$

すなわち左辺は奇数、右辺は偶数となり、矛盾を生じる。

ゆえに a と b のうち一方は偶数であり、他方は奇数である。このとき c^2 は奇数なので、 c も奇数である。□

考察の対象となるピタゴラス数 (a, b, c) の満たすべき条件を、ここで改めて整理する。

- (1) $a^2 + b^2 = c^2$ を満たす。
- (2) a, b, c は互いに素である。
- (3) a は奇数、 b は偶数である。

2.2 ピタゴラス数の生成

定理 2.2.1 任意の既約ピタゴラス数 (a, b, c) について、 $c+b$ と $c-b$ は互いに素で、共に奇数の二乗である。

証明 (2.1.1) は

$$a^2 = c^2 - b^2 = (c+b)(c-b) \quad (2.2.1)$$

と書き直される。いま、 d を $c+b$ と $c-b$ の公約数とすれば、

$$(c+b) + (c-b) = 2c, \quad (c+b) - (c-b) = 2b$$

は共に d で割り切れるが、 b と c は互いに素なので、 d は 2 か 1 でなくてはならない。ところが $d=2$ ならば、(2.2.1) において a^2 は 4 の倍数、よって a は偶数となり、 a が奇数という前提と矛盾する。よって $d=1$ となり、 $c+b$ と $c-b$ は互いに素である。

このとき、(2.2.1) で述べられるように $(c+b)(c-b)$ が奇数の二乗になるには、 $c+b$ と $c-b$ がそれぞれ、それ自体奇数の二乗でなくてはならない。□

定理 2.2.2 既約ピタゴラス数 (a, b, c) は、互いに素である奇数 s と t ($s > t \geq 1$) により、

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2} \quad (2.2.2)$$

として与えられる。

証明 定理 2.1.2 により

$$c + b = s^2, \quad c - b = t^2$$

これを (2.2.1) に代入し、或いは b と c について解いて結論を得る。 □

例 2.2.1 $s \leq 23$ で (2.2.2) を適用した結果を示す。

s	t	a	b	c	s	t	a	b	c
3	1	3	4	5	17	11	187	84	205
5	1	5	12	13	17	13	221	60	229
5	3	15	8	17	17	15	255	32	257
7	1	7	24	25	19	1	19	180	181
7	3	21	20	29	19	3	57	176	185
7	5	35	12	37	19	5	95	168	193
9	1	9	40	41	19	7	133	156	205
9	5	45	28	53	19	9	171	140	221
9	7	63	16	65	19	11	209	120	241
11	1	11	60	61	19	13	247	96	265
11	3	33	56	65	19	15	285	68	293
11	5	55	48	73	19	17	323	36	325
11	7	77	36	85	21	1	21	220	221
11	9	99	20	101	21	5	105	208	233
13	1	13	84	85	21	11	231	160	281
13	3	39	80	89	21	13	273	136	305
13	5	65	72	97	21	17	357	76	365
13	7	91	60	109	21	19	399	40	401
13	9	117	44	125	23	1	23	264	265
13	11	143	24	145	23	3	69	260	269
15	1	15	112	113	23	5	115	252	277
15	7	105	88	137	23	7	161	240	289
15	11	165	52	173	23	9	207	224	305
15	13	195	28	197	23	11	253	204	325
17	1	17	144	145	23	13	299	180	349
17	3	51	140	149	23	15	345	152	377
17	5	85	132	157	23	17	391	120	409
17	7	119	120	169	23	19	437	84	445
17	9	153	104	185	23	21	483	44	485

定理 2.2.3 既約ピタゴラス数は無数に存在する。

証明 定理 2.2.2 において、 $s > t \geq 1$ を満たす互いに素な奇数の組 (s, t) は無数に存在する。 □

2.3 ピタゴラス数と円周上の点

(2.2.1)において、 $a^2 + b^2 = c^2$ の両辺を $c^2 \neq 0$ で割ると

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \quad (2.3.1)$$

なので、有理数の組 $(a/c, b/c)$ は方程式

$$x^2 + y^2 = 1 \quad (2.3.2)$$

の解である。すなわち、 xy 座標で $(a/c, b/c)$ と表される平面上の点は、同じ座標系で(2.3.2)の表す単位円 κ （座標原点が中心で半径1の円）の円周上にある。本節では図形の解釈としてピタゴラス数を見出す方法を考察する。

任意の有理数 q に対し、 κ 上の点 $P(-1, 0)$ を通り傾きが q である直線を λ とすれば、 λ を表す方程式は

$$y = q(x + 1) \quad (2.3.3)$$

である。いま、点 Q において、 λ が再び κ と交わるとする。(2.3.2)と(2.3.3)を連立方程式として解けば、 Q の座標が求められる。二つの方程式から y を消去、整理すると

$$(q^2 + 1)x^2 + 2q^2x + (q^2 - 1) = 0$$

この方程式は $x = -1$ を解に持つので、両辺を $x + 1$ で割って

$$(q^2 + 1)x + (q^2 - 1) = 0 \quad \text{すなわち} \quad x = \frac{1 - q^2}{1 + q^2}$$

このとき(2.3.3)により

$$y = q\left(\frac{1 - q^2}{1 + q^2} + 1\right) = \frac{2q}{1 + q^2}$$

いま、 q は有理数なので、適当な整数 m と n により $q = n/m$ と表される。よって Q の座標は

$$(x, y) = \left(\frac{1 - (n/m)^2}{1 + (n/m)^2}, \frac{2(n/m)}{1 + (n/m)^2}\right) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right) \quad (2.3.4)$$

となり、(2.3.1)と(2.3.4)を比べることで、次の定理を得る。

定理 2.3.1 ピタゴラス数 (a, b, c) は、適当な整数 m と n により、

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2 \quad (2.3.5)$$

として与えられる。

(2.3.5) で与えられるピタゴラス数が既約であるためには、更に次の条件が満たされなくてはならない。

(1) m と n は互いに素である。

(2) m と n のうち、一方は偶数、他方は奇数である。

例 2.3.1 $m \leq 16$ で (2.3.5) を適用した結果を示す。

m	n	a	b	c	m	n	a	b	c
2	1	3	4	5	12	5	119	120	169
3	2	5	12	13	12	7	95	168	193
4	1	15	8	17	12	11	23	264	265
4	3	7	24	25	13	2	165	52	173
5	2	21	20	29	13	4	153	104	185
5	4	9	40	41	13	6	133	156	205
6	1	35	12	37	13	8	105	208	233
6	5	11	60	61	13	10	69	260	269
7	2	45	28	53	13	12	25	312	313
7	4	33	56	65	14	1	195	28	197
7	6	13	84	85	14	3	187	84	205
8	1	63	16	65	14	5	171	140	221
8	3	55	48	73	14	9	115	252	277
8	5	39	80	89	14	11	75	308	317
8	7	15	112	113	14	13	27	364	365
9	2	77	36	85	15	2	221	60	229
9	4	65	72	97	15	4	209	120	241
9	8	17	144	145	15	8	161	240	289
10	1	99	20	101	15	14	29	420	421
10	3	91	60	109	16	1	255	32	257
10	7	51	140	149	16	3	247	96	265
10	9	19	180	181	16	5	231	160	281
11	2	117	44	125	16	7	207	224	305
11	4	105	88	137	16	9	175	288	337
11	6	85	132	157	16	11	135	352	377
11	8	57	176	185	16	13	87	416	425
11	10	21	220	221	16	15	31	480	481
12	1	143	24	145			⋮		

2.4 平方数の和となる素数

最初に定理 2.1.1 で示したように、

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

を満たすピタゴラス数 (a, b, c) のうち、右辺の c は常に奇数である。一般に奇数は、4 を法として (すなわち 4 で割った余りが 1 であるか 3 であるかに応じて)、大きく二つに分類される。

[A] 4 を法として 1 に合同な奇数 $(1, 5, 9, 13, \dots)$

[B] 4 を法として 3 に合同な奇数 $(3, 7, 11, 15, \dots)$

いま、ピタゴラス数を求めるための二つの方法の実例、例 2.2.1 と例 2.3.1 のいずれにおいても、

$$c = 5, 13, 17, 25, 29, \dots \equiv 1 \pmod{4}$$

という結果であり、 c はすべて分類 [A] に属しているように思われる。以下、 c の性質を更に詳しく知るために、どのような数が平方数の和になるのかを問うが、本節では第一段階として、素数の場合に焦点を当てる。素数のうち 2 は

$$2 = 1^2 + 1^2$$

と表されるので、ここからは奇素数 (奇数の素数) を考察の対象とする。

定理 2.4.1 奇素数 p が平方数の和

$$p = a^2 + b^2$$

として表されるならば、 p は 4 を法として 1 に合同である。

証明 a, b の偶奇が一致すれば、 p は明らかに偶数なので、 a を奇数、 b を偶数とする。このとき a, b は整数 α, β により $a = 2\alpha + 1$ 、 $b = 2\beta$ と表されるので、

$$p = (2\alpha + 1)^2 + (2\beta)^2 = 4(\alpha^2 + \beta^2 + \alpha) + 1$$

となる。 □

定理 2.4.2 奇素数 p が 4 を法として 1 に合同ならば、

$$p = a^2 + b^2 \tag{2.4.1}$$

を満たすような整数 a, b が存在する。

証明 考察の出発点として、古典的な数論における中核を成す命題、平方剰余の相互法則の一部を補題とする。補題の証明は本講義の範囲を逸脱するので割愛する。

補題 奇素数 p が 4 を法として 1 に合同である場合、またその場合に限り、

$$a^2 \equiv -1 \pmod{p}$$

となるような整数 a が存在する。

例 2.4.1 補題の合同式は、 $a^2 + 1^2$ が p で割り切れることを意味する。例えば $p = 5$ の場合

$$2^2 + 1^2 = 5 = 1 \times 5, \quad 3^2 + 1^2 = 10 = 2 \times 5$$

$p = 13$ の場合

$$5^2 + 1^2 = 26 = 2 \times 13, \quad 8^2 + 1^2 = 65 = 5 \times 13$$

$p = 17$ の場合

$$4^2 + 1^2 = 17 = 1 \times 17, \quad 13^2 + 1^2 = 170 = 10 \times 17$$

$p = 29$ の場合

$$12^2 + 1^2 = 145 = 5 \times 29, \quad 17^2 + 1^2 = 290 = 10 \times 29$$

など。他方、 $p = 3, 7, 11, 19, 23, \dots$ の場合、与えられた条件を満たす整数 a は存在しない。

補題は与えられた $p \equiv 1 \pmod{4}$ に対し、

$$a^2 + b^2 = kp \tag{2.4.2}$$

となるような整数 a, b, k が存在することを示している（補題の場合は $b = 1$ ）。

以下、これらの数から

$$a'^2 + b'^2 = k'p \quad (k' < k) \tag{2.4.3}$$

となるような整数 a', b', k' を導く、降下法と呼ばれる手続きを示す。

1.

$$\begin{cases} \alpha \equiv a \\ \beta \equiv b \end{cases} \pmod{k}, \quad -\frac{k}{2} \leq \alpha, \beta \leq \frac{k}{2}$$

となるような整数 α, β を求める。

2. $\alpha^2 + \beta^2 \equiv a^2 + b^2 \equiv 0 \pmod{k}$ なので、

$$\alpha^2 + \beta^2 = kk'$$

となるような整数 k' が存在する。

$$k' = \frac{\alpha^2 + \beta^2}{k} \leq \frac{(k/2)^2 + (k/2)^2}{2} = \frac{k}{2}$$

なので、 $k' < k$ である。

3. $a^2 + b^2$ と $\alpha^2 + \beta^2$ の積を考える。定義により

$$(a^2 + b^2)(\alpha^2 + \beta^2) = k^2 k' p$$

である一方、

$$(a^2 + b^2)(\alpha^2 + \beta^2) = (a\alpha + b\beta)^2 + (a\beta - b\alpha)^2$$

は恒等式、ゆえに

$$(a\alpha + b\beta)^2 + (a\beta - b\alpha)^2 = k^2 k' p$$

が成り立つ。

4. $a\alpha + b\beta \equiv aa + bb = a^2 + b^2 \equiv 0$, $a\beta - b\alpha \equiv ab - ba = 0 \pmod{k}$ なので、

$$a' = \frac{a\alpha + b\beta}{k}, \quad b' = \frac{a\beta - b\alpha}{k}$$

となるような整数 a', b' が存在する。このとき $(ka')^2 + (kb')^2 = k^2 k' p$ 、
従って式 (2.4.3) :

$$a'^2 + b'^2 = k' p \quad (k' < k)$$

を得る。

$k' = 1$ ならば、式 (2.4.1) が成り立っていることになる。 $k' \geq 2$ ならば、 a', b', k' をそれぞれ a, b, k と読み替えて、同じ手続きを繰り返せばよい。□

例 2.4.2 例 2.4.1 で挙げた

$$12^2 + 1^2 = 5 \times 29 \tag{2.4.4}$$

に、降下法の手続きを適用してみる。 $12 \equiv 2$, $1 \equiv 1 \pmod{5}$ より

$$2^2 + 1^2 = 5 \times 1$$

よって

$$(12^2 + 1^2)(2^2 + 1^2) = 5^2 \times 1 \times 29$$

他方

$$\begin{aligned} (12^2 + 1^2)(2^2 + 1^2) &= (12 \times 2 + 1 \times 1)^2 + (12 \times 1 - 1 \times 2)^2 \\ &= 25^2 + 10^2 = (5 \times 5)^2 + (5 \times 2)^2 \end{aligned}$$

ゆえに $(5 \times 5)^2 + (5 \times 2)^2 = 5^2 \times 1 \times 29$ 、すなわち

$$5^2 + 2^2 = 29 \tag{2.4.5}$$

を得る。

2.5 平方数の和となる合成数

定理 2.5.1 整数 n が整数 k と r 個の相異なる素数 p_1, \dots, p_r により

$$n = k^2 p_1 p_2 \dots p_r$$

と分解されるとき、これらの素数がすべて、2 に等しいか、4 を法として 1 に合同であれば、 n は平方数の和として表される。

証明 前節における考察によれば、「素数 p が平方数の和 $a^2 + b^2$ として表される」ことは、「素数 p が 2 に等しいか、4 を法として 1 に合同である」とこと同値である。いま、与えられた r 個の素数がこれらの条件を満たすとし、このうち p_i, p_j ($1 \leq i \neq j \leq r$) がそれぞれ

$$p_i = a_i^2 + b_i^2, \quad p_j = a_j^2 + b_j^2$$

と表されるとすれば、命題 2.4.2 の証明における降下法で用いられた恒等式により、積 $p_i p_j$ も平方数の和として

$$\begin{aligned} p_i p_j &= (a_i^2 + b_i^2)(a_j^2 + b_j^2) \\ &= (a_i a_j + b_i b_j)^2 + (a_i b_j - b_i a_j)^2 \end{aligned}$$

と表される。この新たな平方数の和は、別の素数 $p_k = a_k^2 + b_k^2$ と共に、更に新たな平方数の和を生成する。こうして素数の積 $p_1 p_2 \dots p_r$ は最終的に平方数の和 $a^2 + b^2$ として表されるので、 n は

$$n = (ka)^2 + (kb)^2$$

と表される。 □

例 2.5.1 $1885 = 5 \times 13 \times 29$ の素因数 5, 13, 29 はすべて 4 を法として 1 に合同なので、1885 は平方数の和として表される。

$$5 \times 13 = (1^2 + 2^2)(2^2 + 3^2) = (2 + 6)^2 + (3 - 4)^2 = 8^2 + 1^2$$

または

$$5 \times 13 = (2^2 + 1^1)(2^2 + 3^2) = (4 + 3)^2 + (6 - 2)^2 = 7^2 + 4^2$$

$5 \times 13 = 8^2 + 1^2$ から

$$5 \times 13 \times 29 = (8^2 + 1^2)(2^2 + 5^2) = (16 + 5)^2 + (40 - 2)^2 = 21^2 + 38^2$$

または

$$5 \times 13 \times 29 = (1^2 + 8^2)(2^2 + 5^2) = (2 + 40)^2 + (5 - 16)^2 = 42^2 + 11^2$$

$5 \times 13 = 7^2 + 4^2$ から

$$5 \times 13 \times 29 = (7^2 + 4^2)(2^2 + 5^2) = (14 + 20)^2 + (35 - 8)^2 = 34^2 + 27^2$$

または

$$5 \times 13 \times 29 = (4^2 + 7^2)(2^2 + 5^2) = (8 + 35)^2 + (20 - 14)^2 = 43^2 + 6^2$$

このように、1885 は平方数の和として

$$1885 = 11^2 + 42^2 = 21^2 + 38^2 = 27^2 + 34^2 = 43^2 + 6^2$$

と表される。

改めてピタゴラス数 (a, b, c) に立ち返る。

定理 2.5.2 ピタゴラス数 (a, b, c) の c は、4 を法として 1 と合同な素数の積 (素数が一つだけの場合も含む) である。

証明 定理 2.2.2 によれば、 (a, b, c) は互いに素であるような二つの奇数 $s > t \geq 1$ により

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

として生成されるのだった。このとき平方数の和 $s^2 + t^2$ は $2c$ に等しいので、定理 2.5.1 により、 c は 4 を法として 1 と合同な素数の積である。 \square

例 2.5.2 $c = 1885 = 5 \times 13 \times 29$ となるようなピタゴラス数 (a, b, c) を求める。

[1] $c = 1885 = 11^2 + 42^2$ から

$$2 \times 1885 = (1^2 + 1^2)(11^2 + 42^2) = (11 + 42)^2 + (42 - 11)^2 = 53^2 + 31^2$$

なので

$$a = 53 \times 31 = 1643, \quad b = \frac{53^2 - 31^2}{2} = 924$$

[2] $c = 1885 = 21^2 + 38^2$ から

$$2 \times 1885 = (1^2 + 1^2)(21^2 + 38^2) = (21 + 38)^2 + (38 - 21)^2 = 59^2 + 17^2$$

なので

$$a = 59 \times 17 = 1003, \quad b = \frac{59^2 - 17^2}{2} = 1596$$

[3] $c = 1885 = 27^2 + 34^2$ から

$$2 \times 1885 = (1^2 + 1^2)(27^2 + 34^2) = (27 + 34)^2 + (34 - 27)^2 = 61^2 + 7^2$$

なので

$$a = 61 \times 7 = 427, \quad b = \frac{61^2 - 7^2}{2} = 1836$$

[4] $c = 1885 = 43^2 + 6^2$ から

$$2 \times 1885 = (1^2 + 1^2)(43^2 + 6^2) = (43 + 6)^2 + (6 - 43)^2 = 49^2 + 37^2$$

なので

$$a = 49 \times 37 = 1813, \quad b = \frac{49^2 - 37^2}{2} = 516$$

以上により、求めるピタゴラス数は

$$(427, 1836, 1885), \quad (1003, 1596, 1885),$$

$$(1643, 924, 1885), \quad (1813, 516, 1885)$$

である。

2.6 フェルマーの定理

これまで見てきた通り、方程式

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

の整数解は無数に存在する。これに対し、 n を 2 より大きい整数として、

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

の整数解は ($x = z, y = 0$ のような自明な解を除いて) 存在するのか。

微積分の先駆となる業績を残すなど、卓越した数学者でもあったフランスの法律家 Pierre de Fermat (1601-1665) は、蔵書の余白に「(そのような数が存在しないことについて) 私は実に驚くべき証明を発見したが、余白が狭くて収め切れない」と記した。フェルマーによる証明は、今日なお見出されていない。

数学の知識を特段必要としない内容の単純さに関わらず、フェルマーの問題は後世の優れた数学者たちの挑戦を退け続け、完全な解決はフェルマーの死後、三世紀以上も後の 1995 年、イギリスの数学者 Andrew Wiles によって初めて与えられた。

最先端の現代数学に基づくワイルズの証明は、本講義の範囲を遥かに逸脱する。ここでは本章における探求の集大成として、フェルマー自身による $n = 4$ の場合の証明を、現代風の語法に翻訳して紹介する。なお、以下の命題では z の指数が 2 になっているが、 z が平方数 ζ^2 に等しければ、方程式は $x^4 + y^4 = \zeta^4$

と書かれるので、ここでは本来のフェルマーの定理よりも、より強い主張が為されていることになる。

定理 2.6.1 方程式

$$x^4 + y^4 = z^2 \quad (2.6.1)$$

の整数解は存在しない。

証明 与えられた方程式が正の整数解 (X_0, Y_0, Z_0) を持つと仮定し、降下法により矛盾を導く。

$a = X_0^2$, $b = Y_0^2$, $c = Z_0$ とおけば (a, b, c) はピタゴラス数なので、

$$X_0^2 = a = st, \quad Y_0^2 = b = \frac{s^2 - t^2}{2}, \quad Z_0 = c = \frac{s^2 + t^2}{2}$$

となるような、互いに素な二つの奇数 $s > t \geq 1$ が存在する。

$X_0^2 = a$ は奇数の平方数なので $st \equiv 1 \pmod{4}$ 、従って s と t は 4 を法として、共に 1 に合同か、共に 3 に合同か、いずれにせよ $s \equiv t \pmod{4}$ で、 $s - t$ は 4 で割り切れる。

$2Y_0^2 = s^2 - t^2 = (s - t)(s + t)$ については、 s と t が互いに素な奇数なので、 $s - t$ と $s + t$ の最大公約数は 2 である。 $s - t$ は 4 で割り切れるので、 $s + t$ は奇数の 2 倍となる。また $s - t$ と $s + t$ の積は平方数の 2 倍である。以上の条件が成り立つには、互いに素な二つの奇数 u, v が存在して

$$\begin{cases} s - t = 4u^2 \\ s + t = 2v^2 \end{cases} \quad \text{すなわち} \quad \begin{cases} s = 2u^2 + v^2 \\ t = -2u^2 + v^2 \end{cases}$$

が成り立たなくてはならない。このとき $X_0^2 = st = -4u^2 + v^2$ 、すなわち

$$X_0^2 + 4u^4 = v^4$$

$a' = X_0$, $b' = 2u^2$, $c' = v^2$ とおけば、 (a', b', c') はピタゴラス数なので、

$$X_0 = a' = s't', \quad 2u^2 = b' = \frac{s'^2 - t'^2}{2}, \quad v^2 = c' = \frac{s'^2 + t'^2}{2}$$

となるような、互いに素な二つの奇数 $s' > t' \geq 1$ が存在する。

$4u^2 = s'^2 - t'^2 = (s' - t')(s' + t')$ について、 s' と t' が互いに素な奇数なので、 $s' - t'$ と $s' + t'$ の最大公約数は 2 である。また $s' - t'$ と $s' + t'$ の積は平方数である。以上の条件が成り立つには、互いに素な二つの奇数 X_1, Y_1 が存在して

$$\begin{cases} s' - t' = 2X_1^2 \\ s' + t' = 2Y_1^2 \end{cases} \quad \text{すなわち} \quad \begin{cases} s' = X_1^2 + Y_1^2 \\ t' = -X_1^2 + Y_1^2 \end{cases}$$

が成り立たなくてはならない。このとき

$$v^2 = \frac{s'^2 + t'^2}{2} = \frac{(X_1^2 + Y_1^2)^2 + (-X_1^2 + Y_1^2)^2}{2} = X_1^4 + Y_1^4$$

なので、 $Z_1 = v$ とおけば、 (X_1, Y_1, Z_1) もまた、方程式 (2.6.1) の整数解となる。
元の解 (X_0, Y_0, Z_0) と、そこから派生した新たな解 (X_1, Y_1, Z_1) を比較すると、

$$Z_0 = \frac{s^2 + t^2}{2} = \frac{(2u^2 + v^2)^2 + (-2u^2 + v^2)^2}{2} = 4u^4 + v^4 = 4u^4 + Z_1^4$$

で、明らかに $Z_0 > Z_1$ である。

同様の理由で、任意の自然数 $k = 1, 2, \dots$ に対し、方程式 (2.6.1) の正の整数解 (X_k, Y_k, Z_k) からは別の正の整数解 $(X_{k+1}, Y_{k+1}, Z_{k+1})$ が導かれ、

$$Z_0 > Z_1 > Z_2 > \dots > Z_k > Z_{k+1} > \dots$$

という無限の系列が生じることになるが、これは方程式の解がすべて正の整数であるという前提と矛盾する。 \square

Aperçu du cours du tronc commun : *Redécouvrons les Mathématiques*

KUKITA Eishi

Mots-clefs : programme du premier cycle, éducation des mathématiques,
histoire des mathématiques, arithmétique, géométrie

Le cours intitulé : *Redécouvrons les Mathématiques — Merveilles des Nombres et des Figures*, a été conçu dans le cadre du tronc commun lors de la réforme de notre faculté de l'année 2019. Il a pour but principal de procurer à nos étudiantes la joie intellectuelle de découvrir par elles-mêmes, à travers les activités manuelles comme calculs et constructions et les raisonnements appuyés sur le résultat de ces travaux, de belles propriétés inattendues, recelées dans les nombres et les figures apparemment sans aucun mystère. En guise d'aperçu de ce cours, cet article se propose d'en mettre en ordre axiomatiquement les matériels, puisés dans l'histoire de l'arithmétique et de la géométrie.