P-1

正則素数の場合のフェルマーの最終定理
Fermat's Last Theorem for Regular Primes

○吉田佳祐 [1]
Keisuke Yoshida

Abstract: We prove Fermat's Last Theorem when the exponent is a regular prime, following Kummer's ideas.

1. フェルマーの最終定理

定理 1 (Wiles, Taylor–Wiles)**.** 自然数 $n \geq 3$ に対し

$$x^n + y^n = z^n, xyz \neq 0 \tag{1}$$

を満たす有理整数の組 (x, y, z) は存在しない.

n が奇素数の場合と 4 の場合を証明すれば十分なこと，及び x, y, z のどの 2 つも互いに素である場合の非存在性を示せば十分なことは明らかである．また，$n = 3, 4$ の場合はフェルマーやオイラーによって証明されている．よって，n が 5 以上の素数 p である場合を考えればよい．本稿では，p が正則素数と呼ばれる素数のときの Kummer の証明を扱う．$p \nmid xyz$ の時は比較的楽なので，x, y, z の対称性から次の定理を証明するのが目標となる．

定理 2. p を 5 以上の正則素数とする. このとき

$$x^p + y^p = z^p, p \nmid xy, p \mid z, z \neq 0, \gcd(x, y, z) = 1 \tag{2}$$

を満たす有理整数の組 (x, y, z) は存在しない.

2. 円分体の理論の紹介

定義 3. $\mathbb{Q}$ の有限次拡大を **代数体** という .
$\mathfrak{o} := \{\alpha \in \mathbb{C} : \alpha$は最高次係数が 1 の整数係数多項式の根 $\}$,
代数体 K に対し $\mathfrak{o}_K := K \cap \mathfrak{o}$ を $\boldsymbol{K}$ **の整数環** という.
$\left\{(\mathfrak{a})^{-1}\mathfrak{b} : \mathfrak{a}, \mathfrak{b} \neq 0$ は $\mathfrak{o}_K$のイデアル$\right\} \Big/ \{\alpha\mathfrak{o}_K : \alpha \in K^*\}$
を H_K と書き, $\boldsymbol{K}$ **のイデアル類群** という. H_K は有限群となることが知られており, $h_K := |H_K|$ を $\boldsymbol{K}$ **の類数** という.

以下 p を奇素数, ζ を $e^{2\pi i/p}$ と固定する.

補題 4. $\mathbb{Q}(\zeta)$ とその最大実部分体 $\mathbb{Q}(\zeta)^+$ の整数環はそれぞれ $\mathbb{Z}[\zeta]$, $\mathbb{Z}[\zeta + \zeta^{-1}]$ である.

以下 h_p を $\mathbb{Q}(\zeta)$ の類数, h_p^+ を $\mathbb{Q}(\zeta)^+$ の類数とする.

定義 5. $p \nmid h_p$ となる素数 p を **正則素数** という.

定理 6. $h_p^+ \mid h_p$.

補題 7. $p \nmid h_p^+$, $\alpha \in \mathbb{Z}[\zeta]_{(1-\zeta)}$ は法 $(1-\zeta)^p$ で 1 に合同, $\overline{\alpha} = \alpha^{-1}$, $(\alpha) = (\mathbb{Q}(\zeta)$ のイデアル$)^p \Rightarrow \alpha = (\mathbb{Q}(\zeta)$ の元$)^p$.

定理 8 (Kummer の補題)**.** p : 正則素数, $\varepsilon \in \mathbb{Z}[\zeta]^\times$, ε は法 p で有理整数に合同. $\Rightarrow \varepsilon = (\mathbb{Q}(\zeta)$ の元$)^p$.

3. 正則素数の場合のフェルマーの最終定理の証明

以下 $\lambda := (1-\zeta)(1-\zeta^{-1})$ とする. (x, y, z) が (2) を満たすとし, $a := z$ を割り切る p の最高冪, $m := \frac{ap(p-1)}{2}$, $\eta := \frac{p^{ap}}{\lambda^m}$, $(\omega, \theta, \xi) := (x, y, \frac{z}{p^a})$ とすると $(p)_{\mathbb{Z}[\lambda]} = (\lambda)_{\mathbb{Z}[\lambda]}^{\frac{p-1}{2}}$ だから $\eta \in \mathbb{Z}[\lambda]^\times$ となり次の定理に矛盾し, 定理 2 が示される.

定理 9. p を 5 以上の正則素数とする. このとき

$$\omega^p + \theta^p = \eta\lambda^m\xi^p \tag{3}$$

を満たす $\mathbb{Z}[\lambda] \setminus \{0\}$ の元の組 (ω, θ, ξ) と $\eta \in \mathbb{Z}[\lambda]^\times$ と $m \in \mathbb{Z}$ は存在しない. ただし $\frac{p(p-1)}{2} \leq m$, $\eta \in \mathbb{Z}[\lambda]^\times$, $\lambda, \omega, \theta, \xi \in \mathbb{Z}[\lambda]$ のどの 2 元も単位イデアルを生成する.

Proof. 解が存在するとする. 法 p で異なる $a, b \in \mathbb{Z}$ に対し, $\mathfrak{p} \mid (\omega + \zeta^a\theta), (\omega + \zeta^b\theta)$ となる $\mathbb{Z}[\zeta]$ の素イデアル $\mathfrak{p}$ が存在するならば, $\omega + \zeta^a\theta - (\omega + \zeta^b\theta) = \zeta^a \frac{1-\zeta^{b-a}}{1-\zeta}(1-\zeta)\theta$, $\zeta^{b-a}(\omega + \zeta^a\theta) - (\omega + \zeta^b\theta) = -\frac{1-\zeta^{b-a}}{1-\zeta}(1-\zeta)\omega$ より, $\mathfrak{p} = (1-\zeta)$. また $(\lambda) = (1-\zeta)^2$, $(\lambda, \theta) = (1)$ より $\theta \notin (1-\zeta)$ なので $(\omega + \zeta^a\theta) + (\omega + \zeta^b\theta) = (1-\zeta)$. 従って $(1-\zeta)^2 = (\lambda)$ で割り切れるような $(\omega + \zeta^a\theta)$ は高々一つしかない. 一方 p は $\mathbb{Z}[\zeta]$ で完全分岐するから $\mathbb{Z}[\lambda]/(\lambda) \cong \mathbb{Z}/p\mathbb{Z}$ なので, $\omega + \theta \equiv 0 \pmod{(\lambda)}$. つまり (λ) で割り切れるものは $(\omega + \theta)$ のみで, $1 \leq a \leq p-1$ に対し $(\omega + \zeta^a\theta)$ は $(1-\zeta) = (1-\zeta^a)$ で 1 回だけ割る. 従って $(\omega + \theta)\displaystyle\prod_{a=1}^{p-1} \frac{\omega + \zeta^a\theta}{1-\zeta^a} = (\text{単数})\lambda^{m-\frac{p-1}{2}}\xi^p$ に素イデアル分解の一意性を使うと, 次を満たす $\mathbb{Z}[\zeta]$ のイデアル $B_a (0 \leq a \leq p-1)$ が存在する.

$$\left(\frac{\omega + \zeta^a\theta}{1-\zeta^a}\right) = B_a^p \ (1 \leq a \leq p-1), \tag{4}$$

$$(\omega + \theta) = (\lambda)^{m-\frac{p-1}{2}} B_0^p, \tag{5}$$

$$(\xi) = B_0 B_1 \cdots B_{p-1}, \tag{6}$$

$$(1-\zeta) \nmid B_i (i = 0, 1, 2, \cdots, p-1). \tag{7}$$

(5) より B_0^p は $\mathbb{Q}(\zeta)^+ \cap \mathbb{Z}[\zeta] = \mathbb{Z}[\lambda]$ の元で生成される. $\mathbb{Q}(\zeta)^+$ の違うイデアルは延長すると違う $\mathbb{Q}(\zeta)$ のイデアルとなるため, この元は $B_0^p \cap \mathbb{Q}(\zeta)^+$ も生成する. 更に p は正則素数だから定理 6 より, $p \nmid h_p^+$. よって $pk + lh_p^+ = 1$ となる $k, l \in \mathbb{Z}$ があり

$$(B_0 \cap \mathbb{Q}(\zeta)^+)^1 = (B_0 \cap \mathbb{Q}(\zeta)^+)^{pk} (B_0 \cap \mathbb{Q}(\zeta)^+)^{lh_p^+}$$

よりこれも単項イデアル. $\overline{B_0^p} = B_0^p$ と素イデアル分解の一意性より $\overline{B_0} = B_0$ なので, (7) と $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)^+] = 2$ より, $B_0 \cap \mathbb{Q}(\zeta)^+$ の生成元 ρ_0 が B_0 も生成する. 従って

1: 日大理工・院 (前)・数学

$$\omega+\theta=\eta_0\lambda^{m-\frac{p-1}{2}}\rho_0^p \tag{8}$$

を満たす $\eta_0\in\mathbb{Z}[\lambda]^\times$ がある. $a\not\equiv 0\pmod p$ に対し $\alpha_a:=\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\right)^{-1}$ とすると

$$\begin{aligned}\alpha_a &= \frac{1-\zeta^{-a}}{1-\zeta^a}\times\frac{\omega+\zeta^a\theta}{\omega+\zeta^{-a}\theta}-1+1\\ &= -\zeta^{-a}\times\frac{\omega(1-\zeta^a)+\zeta^a(\omega+\theta)}{\omega(1-\zeta^{-a})+\zeta^{-a}(\omega+\theta)}-1+1\\ &= -\frac{(1+\zeta^{-a})(\omega+\theta)}{\omega(1-\zeta^{-a})+\zeta^{-a}(\omega+\theta)}+1\end{aligned}$$

となり, $(\lambda)=(1-\zeta)^2$, $(\lambda,\omega)=(1)$, (5) より α_a は法 $(1-\zeta)^{2m-p}$ で 1 に合同. $m\geq\frac{p(p-1)}{2}$ から $2m-p\geq p$ なので, 特に $\alpha_a\equiv 1\pmod{(1-\zeta)^p}$. α_a の定義と (4) から $\overline{\alpha_a}=\alpha_a^{-1}$, $(\alpha_a)=(\frac{B_a}{B_{-a}})^p$. 補題 7 より次を満たす $\alpha_a'\in\mathbb{Q}(\zeta)$ がある.

$$\alpha_a=\alpha_a'^p. \tag{9}$$

一方 $\frac{\omega+\zeta^a\theta}{1-\zeta^a}\times\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\in\mathbb{Z}[\zeta]$ は複素共役で不変だから $\mathbb{Z}[\lambda]$ の元. (4) より $\mathbb{Z}[\zeta]$ の単項イデアル $(B_aB_{-a})^p$ は, $Z[\lambda]$ の元で生成されているため, B_0 のときと同様に

$$\frac{\omega+\zeta^a\theta}{1-\zeta^a}\times\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}=\eta_a'\beta_a^p \tag{10}$$

となる $\eta_a'\in\mathbb{Z}[\lambda]^\times$, $\beta_a\in\mathbb{Z}[\lambda]$ がある. (9), (10) より

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)^2=\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\right)\alpha_a=\eta_a'(\alpha_a'\beta_a)^p$$

を得るので, これを $\frac{p+1}{2}$ 乗し, $\gamma_a=\frac{\omega+\zeta^a\theta}{1-\zeta^a}$ とすると

$$\gamma_a^p\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right) = \eta_a'^{\frac{p+1}{2}}\left((\alpha_a'\beta_a)^{\frac{p+1}{2}}\right)^p. \tag{11}$$

$\rho_a:=(\alpha_a'\beta_a)^{\frac{p+1}{2}}\gamma_a^{-1}\in\mathbb{Z}[\zeta]$, $\eta_a:=\eta_a'^{\frac{p+1}{2}}\in\mathbb{Z}[\lambda]^\times$ とすると

$$\frac{\omega+\zeta^a\theta}{1-\zeta^a}=\eta_a\rho_a^p. \tag{12}$$

$\eta_{-a}'=\eta_a'$ より $\eta_a=\eta_{-a}$ なので, (12) から $\eta_a\overline{\rho_a}^p=\eta_a\rho_{-a}^p$ だから, $\overline{\rho_a}^p=\rho_{-a}^p$. $p\geq 5$ より $a\not\equiv\pm b\pmod p$ となる $b\in\mathbb{Z}\setminus p\mathbb{Z}$ をとれば, (12), $\eta_a=\eta_{-a}$, $\overline{\rho_a}^p=\rho_{-a}^p$ によって

$$\omega+\zeta^d\theta = (1-\zeta^d)\eta_d\rho_d^p \quad , \tag{13}$$

$$\omega+\zeta^{-d}\theta = (1-\zeta^{-d})\eta_d\overline{\rho_d}^p \tag{14}$$

が成立し $(d=a,b)$, (13) × (14), (8) の両辺の 2 乗は

$$\omega^2+\theta^2+(\zeta^d+\zeta^{-d})\omega\theta = \lambda_d\eta_d^2(\rho_d\overline{\rho_d})^p, \tag{15}$$

$$\omega^2+\theta^2+2\omega\theta = \lambda^{2m-p+1}\eta_0^2\rho_0^{2p}. \tag{16}$$

ただし $\lambda_d=(1-\zeta^d)(1-\zeta^{-d})=2-(\zeta^d+\zeta^{-d})$.

更に $\left(\frac{(15)_{d=a}-(16)}{\lambda_a}-\frac{(15)_{d=b}-(16)}{\lambda_b}\right)\frac{1}{\eta_b^2}=0$ より

$$\left(\frac{\eta_a}{\eta_b}\right)^2(\rho_a\overline{\rho_a})^p+(-\rho_b\overline{\rho_b})^p=\delta_{ab}\lambda^{2m-p}(\rho_0^2)^p. \tag{17}$$

ここで $\delta_{ab}=\left(\frac{\eta_0}{\eta_b}\right)^2\lambda(\lambda_a^{-1}-\lambda_b^{-1})$ で, $a,\ b\not\equiv 0\pmod p$, $a\not\equiv\pm b\pmod p$, λ, λ_a^{-1}, $\lambda_b^{-1}\in\mathbb{Q}(\zeta)^+$, $\left(\frac{\eta_a}{\eta_b}\right)^2\in\mathbb{Z}[\lambda]^\times$ と

$$\begin{aligned}\lambda_a^{-1}-\lambda_b^{-1} &= \frac{\lambda_b-\lambda_a}{\lambda_a\lambda_b}=\frac{2-\zeta^b-\zeta^{-b}-2+\zeta^a+\zeta^{-a}}{\lambda_a\lambda_b}\\ &= \frac{\zeta^{-a}(1-\zeta^{a-b})(1-\zeta^{a+b})}{(1-\zeta^a)(1-\zeta^{-a})(1-\zeta^b)(1-\zeta^{-b})}\\ &= \frac{\zeta^{-a}(1-\zeta)}{\lambda(1-\zeta^a)}\frac{1-\zeta^{-1}}{1-\zeta^{-a}}\frac{1-\zeta^{a-b}}{1-\zeta^{-b}}\frac{1-\zeta^{a+b}}{1-\zeta^b}\end{aligned}$$

$=\frac{(\text{単数})}{\lambda}$ より $\delta_{ab}\in\mathbb{Z}[\lambda]^\times$. (12) と (5) より

$$\begin{aligned}\eta_a &= \frac{\omega+\zeta^a\theta}{1-\zeta^a}\times\rho_a^{-p}=\frac{\omega(1-\zeta^a)+\zeta^a\omega+\zeta^a\theta}{1-\zeta^a}\times\rho_a^{-p}\\ &= \left(\omega+\zeta^a\frac{\omega+\theta}{1-\zeta^a}\right){\rho_a}^{-p}\equiv\omega{\rho_a}^{-p}\pmod{(1-\zeta)^{2m-p}}.\end{aligned}$$

(12) より $(1-\zeta)\nmid\rho_a$ で $2m-p\geq p-1$, $(p)=(1-\zeta)^{p-1}$ より $\eta_a\equiv\omega{\rho_a}^{-p}\pmod p$. b についても同様のため,

$$\frac{\eta_a}{\eta_b}\equiv\left(\frac{\rho_b}{\rho_a}\right)^p\pmod p. \tag{18}$$

$\frac{\rho_b}{\rho_a}\in\mathbb{Z}[\zeta]_{(1-\zeta)}$ は $\sum_{i=0}^{p-2}\frac{b_i}{c_i}\zeta^i(b_i\in\mathbb{Z}, c_i\notin p\mathbb{Z})$ と書けるから

$$\frac{\eta_a}{\eta_b}\equiv\sum_{i=0}^{p-2}\left(\frac{b_i}{c_i}\zeta^i\right)^p=\sum_{i=0}^{p-2}\left(\frac{b_i}{c_i}\right)^p\equiv\text{有理整数}\pmod p. \tag{19}$$

$\frac{\eta_a}{\eta_b}\in\mathbb{Z}[\lambda]^\times$ と (19) が成立するため定理 8 より $\varepsilon^p=\frac{\eta_a}{\eta_b}$ となる $\varepsilon\in\mathbb{Q}(\zeta)$ がある. 実数方程式 $x^p-\frac{\eta_a}{\eta_b}=0$ は p が奇数だから実根を持つので, 根 $\varepsilon,\varepsilon\zeta,\varepsilon\zeta^2,\cdots,\varepsilon\zeta^{p-1}\in\mathbb{Q}(\zeta)$ の中に実数がある. それを改めて ε と置けば, $\varepsilon\in\mathbb{Q}(\zeta)^+$ より $\varepsilon\in\mathbb{Z}[\lambda]^\times$. $\omega_1:=\varepsilon^2\rho_a\overline{\rho_a}$, $\theta_1:=-\rho_b\overline{\rho_b}$, $\xi_1:=\rho_0^2\in\mathbb{Z}[\lambda]$ とおけば (17) より $\omega_1^p+\theta_1^p=\delta_{ab}\lambda^{2m-p}\xi_1^p$. (4), (12), $\overline{\rho_d}^p=\rho_{-d}^p(d=a,b)$, $B_0=(\rho_0)$ から

$$B_a^pB_{-a}^p=(\omega_1)^p,\ B_b^pB_{-b}^p=(\theta_1)^p,\ B_0^2=(\xi_1). \tag{20}$$

(7), $(B_i,\ B_j)=(1)(i\neq j)$, (20) より λ, ω_1, θ_1, $\xi_1\in\mathbb{Z}[\lambda]$ のどの 2 つの元も単位イデアルを生成. $m\leq 2m-p$ より

$$\begin{cases}\omega_1^p+\theta_1^p=\delta_{ab}\lambda^{2m-p}\xi_1^p, \delta_{ab}\in\mathbb{Z}[\lambda]^\times, \frac{p(p-1)}{2}\leq 2m-p\\ \lambda,\ \omega_1,\ \theta_1,\ \xi_1\in\mathbb{Z}[\lambda]\text{ のどの 2 元も }\mathfrak{o}_K\text{を生成.}\end{cases}$$

これで証明冒頭の設定に戻った. 更に $(\xi)=B_0B_1\cdots B_{p-1}$, $(\xi_1)=B_0^2$ より (ξ) の異なる素イデアルの個数は (ξ_1) のそれ以下である. この操作を有限回繰り返すと, (ξ_j) の素イデアルの個数の減少は止まる. それを ξ と置き, 今までの議論を使うと (ξ)=$B_0B_1\cdots B_{p-1}$, (ξ_1)=B_0^2 だが $(B_0,\ B_i)=(1)$ より, $B_1=B_2=\cdots=B_{p-1}=(1)$. 特に $\frac{\omega+\zeta^{\pm1}\theta}{1-\zeta^{\pm1}}\in\mathbb{Z}[\zeta]^\times$ だから, $\alpha_1\in\mathbb{Z}[\zeta]^\times$ となる. α_1 の共役の絶対値は全て 1 だから $\alpha_1=\pm\zeta^c$ となる $c\in\mathbb{Z}$ があり $\alpha_1\equiv 1\pmod{(1-\zeta)^p}$ より, $\alpha_1=1$ が従うから $\frac{\omega+\zeta\theta}{1-\zeta}=\frac{\omega+\zeta^{-1}\theta}{1-\zeta^{-1}}$ を同値変形し

$$\zeta\theta+\zeta\omega=\zeta^{-1}\theta+\zeta^{-1}\omega\Leftrightarrow\zeta(\theta+\omega)=\zeta^{-1}(\theta+\omega). \tag{21}$$

$\theta+\omega=0$ とすると (3) から $\xi=0$ となり矛盾. $\theta+\omega\neq 0$ と (21) から $\zeta^2=1$ となり, $p\geq 5$ に矛盾. □

注意. この証明では波線部でしか p の正則性を使っていないため, 下記の 2 つの条件が満たされれば十分である.

条件 1 ： $p\nmid h_p^+$. $(Vandiver's\,conjecture)$

条件 2 ： $\left(\frac{\eta_a}{\eta_b}\right)^2$ が $\mathbb{Q}(\zeta)^+$ の p 乗数.

$p=257$ のとき $p\mid h_p, p\nmid h_p^+$ となり, 正則素数でなくても条件 1 を満たし得る. また条件 1 の反例はまだ無い.

4. 参考文献

[1] Lawrence C. Washington:"Introduction to Cyclotomic Fields", Second Edition, Graduate Texts in Mathematics, 83, Springer-Verlag, (1997).