# 1　Fermat の最終定理

**Thm 1.1** (Fermat の最終定理)
任意の $n \in \mathbb{N}_{\geq 3}$ に対して，方程式

$$x^n + y^n = z^n, \quad xyz \neq 0$$

の整数解 $(x, y, z)$ は存在しない．

$n$ が奇素数のときのみ示せれば全ての $n \in \mathbb{N}_{\geq 3}$ について示せたことになる．

**Def 1.1** (正則素数)
$\mathbb{Q}(\zeta_p)$ の類数が $p$ で割れない素数 $p$ を正則素数，割れる素数を非正則素数という．

**Thm 1.2**
$p$ を 2 でない正則素数とする．このとき

$$x^n + y^n = z^n, \quad xyz \neq 0$$

の整数解 $(x, y, z)$ で $x, y, z$ が $p$ と互いに素であるものは存在しない．

整数解 $(x, y, z)$ で $x, y, z$ が $p$ と互いに素であるものが存在したとして矛盾を導く．$d := \gcd(x, y)$ が 1 でないときは，$d \mid z$ なので，

$$\left(\frac{x}{d}\right)^n + \left(\frac{y}{d}\right)^n = \left(\frac{z}{d}\right)^n$$

とできる．よって $x, y$ は互いに素としてよい．

$p \geq 5$ とする．$x \equiv y \equiv -z \mod p$ と仮定すると，$-2z^p \equiv z^p \mod p$ つまり，$3z^p \equiv 0 \mod p$ となる．しかし $p \neq 3 \wedge p \nmid z$ よりこれは矛盾．よって $x \equiv y \mod p$ であれば $x \not\equiv -z \mod p$ となるが，方程式を $x^p + (-z)^p = (-y)^p$ と書き換えることによって，$x \not\equiv y \mod p$ としてよい．

$\zeta := \zeta_p$ とおくと，方程式は

$$\prod_{i=0}^{p-1} (x + \zeta^i y) = z^p$$

と表せる．以下，次の STEP に従う．

(STEP1) $i \neq j$ なら，イデアル $(x + \zeta^i y), (x + \zeta^j y)$ は互いに素であることを示す．類数が $p$ と互いに素であることから，$x + \zeta y =$ (単数) $\times$ ($p$ベキ) となる．

(STEP2) $\mathbb{Z}[\zeta]^\times$ の元が，$\zeta$ のベキと $\mathbb{Z}[\zeta]^\times \cap \mathbb{R}$ の元の積であることを示す．このために，全ての共役の絶対値が 1 である代数的整数は 1 のベキ根であることを示す．
(STEP3) $r \in \mathbb{Z}$ により，$x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y \equiv 0 \mod p$ を導き，仮定 $p \nmid x, y$ 使って矛盾を導く．

(STEP1)

**Lem 1.1**
$i \neq j$ なら，イデアル $(x + \zeta^i y), (x + \zeta^j y)$ は互いに素である．

*Proof.* 素イデアル $\mathfrak{P} \subset \mathbb{Z}[\zeta]$ が $(x + \zeta^i y), (x + \zeta^j y)$ を割ると仮定して矛盾を導く． ■

u