フェルマーの平方和定理 （平成２７年）

定義　　m: 平方因子を含まない有理整数

２次体 K の判別式　d　を次のようにする.

$$d = \begin{cases} m & (\ m \equiv 1 \pmod 4\ \text{のとき}\ ) \\ 4m & (\ m \equiv 2,\ 3 \pmod 4\ \text{のとき}\ ) \end{cases}$$

$$\equiv \begin{cases} 1 \pmod 4 \\ 0 \pmod 4 \end{cases}$$

注 1.　　$d = (\omega - \omega')^2$

$\because$　(1)　$m \equiv 2,\ 3 \pmod 4$ のとき

$$\omega = \sqrt{m}, \quad \omega' = -\sqrt{m}$$

$$\therefore\ (\omega - \omega')^2 = 4m$$

(2)　$m \equiv 1 \pmod 4$ のとき

$$\omega = \frac{1 + \sqrt{m}}{2}, \quad \omega' = \frac{1 - \sqrt{m}}{2}$$

$$\therefore\ (\omega - \omega')^2 = m$$

$$\therefore\ d = (\omega - \omega')^2$$

定理１　　p ： 有理奇素数 のとき

$$\left(\frac{d}{p}\right) = 1 \quad \Leftrightarrow \quad p = \pm \pi \cdot \pi' \quad (\ \pi,\ \pi' : \text{同伴でない素数}\ )$$

証 明　　$\left(\frac{d}{p}\right) = 1$　なら　$\left(\frac{m}{p}\right) = 1$

$$a^2 \equiv m \pmod p$$

$$\alpha = a + \sqrt{m} \quad \text{とおく}$$

$$\alpha \cdot \alpha' = a^2 - m \equiv 0 \pmod p \quad \cdots\cdots\cdots\cdots\ (*)$$

$(\ p,\ \alpha\ ) \neq 1$

$\because$　$(\ p,\ \alpha\ ) = 1$　とすると　$(\ p,\ \alpha'\ ) = 1$

$\therefore\ (\ p,\ \alpha \cdot \alpha'\ ) = 1$　…… (*) に矛盾

よって $(\ p,\ \alpha\ ) \neq 1$

p, α を共に割る素数を πとすると　π = (p, α)

p ： 素数ではない

∵ p ： 素数なら p ：π と同伴

∴ p ｜α

∴ p ｜$a + \sqrt{m}$ …… 不可能

∴ $p = \pi \cdot \pi'$　　ただし, π, π' は同伴でない.

∵ π, π' ： 同伴なら

π, π' ｜α, α'

∴ π, π' ｜α － α' = $2\sqrt{m}$

∴ π・π' ｜$2\sqrt{m}$ ・$2\sqrt{m}$

∴ p ｜4 m …… p ∤$2d$ に矛盾

定理 2　$\left(\frac{-4}{p}\right) = 1 \Leftrightarrow p \equiv 1 \ (mod\ 4)$

証明　Q［i］の判別式を d とすると,

d = - 4

p : 奇素数だから

$\left(\frac{-4}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{-1}{p}\right)$

$\left(\frac{4}{p}\right) = 1$　だから

$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

$p \equiv 1 \ (mod\ 4)$ のとき　　$(-1)^{\frac{p-1}{2}} = 1$

∴ $\left(\frac{-4}{p}\right) = 1 \Leftrightarrow p \equiv 1 \ (mod\ 4)$

定理 1 , 定理 2 より, 次の系を得る.

系　　$p \equiv 1 \ (mod\ 4) \Leftrightarrow p = \pi \cdot \pi'$

注 2.　p ： 有理奇素数 のとき

$p = a^2 + b^2$　($a, b \in$ Z)　$\Leftrightarrow$　$p = (a + bi)(a - bi)$　($a, b \in$ Z)

$\Leftrightarrow$　$p = \pi \cdot \pi'$　(π・π' ∈ Q［i］)

系と注 2.より, 次のフェルマーの平方和定理を得る.

定理 3.　　p ： 有理奇素数 のとき

$p = a^2 + b^2$　($a, b \in$ Z)　$\Leftrightarrow$　$p \equiv 1 \ (mod\ 4)$

引用文献

素数と２次体の整数論　　青 木　昇　著　　共立出版　　２０１３