解析学概論　解答例

2019.01.21

■　p を素数，n を整数とする．このとき，命題「n^2 が p で整除できるならば，n は p で整除できる」ことを，背理法および対偶を用いて証明せよ．

(解) 命題 (P)「a，b を整数，p を素数とする．$a\,b$ が p で整除できるならば，a または b は p で整除できる」[*1]が示されていることを前提に証明を行う．

背理法：命題「n^2 が p で整除でき，かつ，n は p で整除できない」と仮定する．n を p で割ったときの商を $m \in \mathbb{Z}$，余りを $\ell \in \mathbb{Z}$ とすると，$0 < \ell < p$ であり，$n = m\,p + \ell$ と表せる．n^2 が p で整除できるので，

$$n^2 = (m\,p + \ell)^2 = (m^2\,p + 2\,m\,\ell)\,p + \ell^2$$

より ℓ^2 は p で整除できる．命題 (P) より ℓ は p で整除でき，これは $0 < \ell < p$ に反する．

対偶：命題「n が p で整除できないならば，n^2 は p で整除できない」を示す．n を p で割ったときの商を $m \in \mathbb{Z}$，余りを $\ell \in \mathbb{Z}$ （$0 < \ell < p$）とする．このとき，$n = m\,p + \ell$ より

$$n^2 = (m\,p + \ell)^2 = (m^2\,p + 2\,m\,\ell)\,p + \ell^2$$

となる．ℓ^2 が p で整除できると仮定すると，命題 (P) により ℓ が p で整除できることになり，これは $0 < \ell < p$ に反する．したがって，ℓ^2 は p で整除できない，つまり，n^2 は p で整除できない．■

[*1] **(証明)**　a が p で整除できるときは明らかに成り立つ．

a が p で整除できないときを考える．$S = \{\, s \in \mathbb{Z} \,|\, a \cdot s \text{ が } p \text{ で整除できる} \,\}$ とする．$p \in S$ より $s_0 = \min\{\, s \in S \,|\, s \geq 1 \,\}$ が存在する．ここで，ある $s \in S$ は s_0 で整除できないと仮定する．s を s_0 で割ったときの商を q，余りを r とすると，$s = s_0 \cdot q + r$，$0 < r < s_0$ と表せる．$s \in S$，$s_0 \in S$ だから，$a \cdot r = a \cdot s - q \cdot (a \cdot s_0)$ より $a \cdot r$ は p で整除できるので，$r \in S$ となり，s_0 の最小性に反する．したがって，すべての $s \in S$ は s_0 で整除できる．$a \cdot b$ と $a \cdot p$ はともに p で整除できるので，$b \in S$，$p \in S$ であるから，b，p は s_0 で整除できる．p は素数だから，$s_0 = 1$ または $s_0 = p$ である．$s_0 = 1$ と仮定すると，$a = a \cdot s_0 \in S$ であるから，a が p で整除できることになり，矛盾である．したがって，$s_0 = p$ となり，b は p で整除できる．■