京都大学　1995 年　入学試験　前期理系数学　問題 2

問題

a，b は $a > b$ をみたす自然数とし，p，d は素数で $p > 2$ とする。このとき，$a^p - b^p = d$ であるならば，d を $2p$ で割った余りが 1 であることを示せ。

解答

初等整数論の基礎を使うと
Fermat の定理より

$$a^p \equiv a \mod p$$
$$b^p \equiv b \mod p$$

したがって
$$a^p - b^p \equiv a - b \mod p$$

つまり
$$d \equiv a - b \mod p$$

また
$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + bp - 1) = d$$

d は素数なので
$$\begin{cases} (a-b) = d \\ (a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + b^{p-1}) = 1 \end{cases} \tag{1}$$

または
$$\begin{cases} (a-b) = 1 \\ (a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + b^{p-1}) = d \end{cases} \tag{2}$$

$(a \geqq 2, b \geqq 1, p > 2)$ なので
$a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + b^{p-1}$ の各項は 1 以上
したがって

$$a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + b^{p-1} > a^{p-1} \geqq 2^2 > 3$$

なので (1) は不可能
(2) を考えると $(a-b) = 1$ より
$$d \equiv 1 \mod p$$

また
$$(a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + b^{p-1}) > 3$$

よりより
$d > 3$ の素数なので d は奇数
したがって $d \equiv 1 \mod 2$
$2, p$ は素数なので 2 と p は互いに素
なので

$$d \equiv 1 \mod 2p$$