# 数チャレ 第94回(2008年11月)

正の整数 $n$ は合成数であり，$n$ と互いに素な任意の整数 $a$ に対して $a^{n-1}-1$ は $n$ で割り切れるとする。

(1) $n$ は奇数であることを示せ。

(2) $n$ は平方数でないことを示せ。

## 解答

(1) $-1$ は $n$ と互いに素であるから，仮定より

$$(-1)^{n-1} \equiv 1 \pmod{n}$$

が成り立つ。ここで，$n$ が偶数であるとすれば $-1 \equiv 1 \pmod{n}$ となるが，$n$ は合成数で $n \geqq 4$ であるからそれは不可能である。よって，$n$ は奇数である。

(証明おわり)

(2) $n$ が平方数であるとすれば，

$$n = m^2 \quad (m \text{ は正の整数})$$

と表される。

$a$ が $n$ と互いに素な整数であるとすれば，

$$gcd(a+m,\ m) = gcd(a,\ m) = 1$$

であるから，仮定より

$$(a+m)^{n-1} \equiv 1 \pmod{n},\quad a^{n-1} \equiv 1 \pmod{n} \qquad \cdots\cdots\ ①$$

一方，二項定理より

$$(a+m)^{n-1} \equiv a^{n-1} + (n-1)a^{n-2}m \pmod{m^2} \qquad \cdots\cdots\ ②$$

①かつ② より，$-a^{n-2}m$ は $m^2 = n$ で割り切れることになるから，

$a^{n-2}$ は $m$ で割り切れる

ことになる。ところが，$a$ と $m$ は互いに素であるから

$$m = 1,\quad n = 1$$

となって，$n$ が合成数(重複も含めて2つ以上の素数の積で表される整数)であることに反する。

よって，$n$ は平方数ではない。 (証明おわり)

(注) このような正の合成数をカーマイケル数(Carmichael number)という。本問では平方数でないことを示したが，実際には平方因数を持たないことが導かれる。$n = 3pq$ とおいて，カーマイケル数の判定条件 Korselt's Criterion から $p=11$，$q=17$ を求めたのが，前回(第93回)の出題内容である。ちなみに，$561 = 3\times11\times17$ は最小のカーマイケル数である。

素数 $p$ に対して，$p$ と互いに素な任意の整数 $a$ が

$$a^{p-1} \equiv 1 \pmod{p}$$

を満たすことは，Fermat の小定理として有名であるが，Carmichael 数の存在は Fermat の小定理が素数判定には使えないことを意味する。