数チャレ 第17回(2002年6月)

pを素数とするとき，次の各命題を証明せよ。

(1) aをpで割り切れない整数とするとき，

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

となる自然数nが存在する。

(2) (1)の条件を満たす最小の自然数nは$p-1$の約数である。

(3) $(p-1)! \equiv -1 \pmod{p}$

コメント：(3)が成り立つことをウィルソン(Wilson)の定理といいます。$(p-1)! \equiv -1 \pmod{p}$を満たす自然数$p$が素数となるのは明らかなので，実は必要十分条件です。

解答

(1) まず，任意の自然数kに対して$a^k \not\equiv 0 \pmod{p}$であることに注意しておく。

pで割った余りは有限個しかないから，

$$a,\ a^2,\ a^3,\ \cdots\cdots,\ a^k,\ \cdots\cdots$$

のうちでpで割った余りが等しいものが存在する。つまり，

$$a^m \equiv a^n \pmod{p}$$

を満たす異なる自然数$m,\ n$が存在する。

$m > n$とするとき，

$$a^{m-n}(a^n - 1) \equiv 0 \pmod{p}, \quad a^{m-n} \not\equiv 0 \pmod{p}$$

より

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

(おわり)

(2) $n = 1$ならば証明は終わっているので，$a \not\equiv 0, 1 \pmod{p}$として集合

$$S_1 = \{a,\ a^2,\ \cdots,\ a^n\} \quad \left(a^n \equiv 1 \pmod{p}\right)$$

を考える。nの最小性より集合S_1の要素は互いに異なり，$\sharp S = n$である。

$2,\ 3,\ \cdots,\ p-1$の中に，pで割った余りがS_1に属するどの数とも異なるものがあればそれをbとし，集合

$$S_2 = \{ab,\ a^2b,\ \cdots,\ a^nb\}$$

を定める。S_2の定め方より

$$\sharp S_2 = n, \quad S_1 \cap S_2 = \varnothing$$

となる。

以下，同様に集合$S_3,\ S_4,\ \cdots$を定めていくと，その作業は有限のr回で終わり，

$$\sharp S_k = n, \quad S_k \cap (S_1 \cup S_2 \cup \cdots \cup S_{k-1}) = \varnothing \quad (k = 3,\ 4,\ \cdots,\ r)$$

を満たすから

$$\sharp S_1 + \sharp S_2 + \cdots + \sharp S_r = nr = p - 1$$

(おわり)

(3) 多項式の一般的性質として，

$$F(X) = X^{p-1} - 1$$
$$= \sum_{k=1}^{p-1} c_k (X-1)(X-2)\cdots(X-k) \qquad (c_{p-1} = 1,\ \ c_k \text{は整数})$$

と表すことができる。(1), (2)より

$$F(2) = 2^{p-1} - 1 = c_1 \equiv 0 \pmod{p}$$
$$F(3) = 3^{p-1} - 1 = 2c_1 + 2c_2 \equiv 0 \pmod{p}$$
$$\vdots$$
$$F(m) = m^{p-1} - 1$$
$$= \sum_{k=1}^{m-1} c_k (m-1)(m-2)\cdots(m-k) \equiv 0 \pmod{p}$$
$$\vdots$$
$$F(p-1) = (p-1)^{p-1} - 1$$
$$= \sum_{k=1}^{p-2} c_k (p-2)(p-3)\cdots(p-1-k) \equiv 0 \pmod{p}$$

であるから，

$$c_1 \equiv c_2 \equiv \cdots \equiv c_{p-2} \equiv 0 \pmod{p}$$
$$X^{p-1} - 1 \equiv (X-1)(X-2)\cdots(X-p+1) \pmod{p}$$

が成り立つ。

$X = 0$ を代入すると

$$-1 \equiv (-1)^{p-1}(p-1)! \pmod{p}$$

p が奇素数のときは，$p-1$ は偶数であるから

$$(p-1)! \equiv -1 \pmod{p}$$

$p = 2$ のときは，直接 $(2-1)! = 1 \equiv -1 \pmod{2}$ が確かめられる。

(おわり)