解答 (2013.10.31 出題)

p を素数とする.

1. $\frac{1}{a} = a$ をみたす $a \in \mathbf{F}_p$ は $a = 1, p-1$ に限ることを示せ.

   $\frac{1}{a} = a$ より $a^2 = 1$. よって $(a-1)(a+1) = 0$, すなわち $(a-1)(a+1) \equiv 0 \bmod p$. よって $a - 1 \equiv 0 \bmod p$ または $a + 1 \equiv 0 \bmod p$. 前者を満たす $a \in \mathbf{F}_p$ は $a = 1$ のみ, 後者を満たす $a \in \mathbf{F}_p$ は $a = p - 1$ のみである.

2. 1. をもちいて, $\mathbf{F}_p$ (p は 3 以上の素数) において $2 \cdot 3 \cdots (p-2) = 1$ (すなわち $(p-2)! \equiv 1 \bmod p$) であることを説明せよ.

   1. より $a = 2, \ldots, p-2$ なら $a \neq \frac{1}{a}$ で, $\frac{1}{a} \neq 1, p-1$ も成り立つので, $\frac{1}{a}$ は $2, \ldots, p-2$ の中にある a と異なる数である. $a \neq b$ なら $\frac{1}{a} \neq \frac{1}{b}$ なので, $\{2, \ldots, p-2\}$ は, $\{a, \frac{1}{a}\}$ なるペアにより重複することなく分けられる. 各ペアの積は 1 なので, $\{2, \ldots, p-2\}$ の積も 1 となる.