問題 (2013.10.31)

学部/学科　　学籍番号　　氏名

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. (ヒント : $\frac{1}{a} = a$ より $a^2 = 1$. よって $(a-1)(a+1) = 0$, すなわち $(a-1)(a+1) \equiv 0 \bmod p$.)

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. (ヒント : 1. より $a = 2, \ldots, p-2$ なら a の逆数は a と等しくない. p は奇数より $2, \ldots, p-2$ は偶数個であることに注意.)