

$$a = (a-b)(a^{p-1} + a^{p-2}b + \dots + ab^{p-2} + b^{p-1})$$

a は素数, $a^{p-1} + a^{p-2}b + \dots + ab^{p-2} + b^{p-1} > 1$, であるから, $a-b=1$, a, b の奇偶は異なる

(i) a が偶数のとき

$$a = a^p - (a-1)^p = -\sum_{k=1}^p pC_k a^{p-k} (-1)^k = -\sum_{k=1}^{p-1} pC_k a^{p-k} (-1)^k + 1 \quad \text{--- (1)}$$

p は奇数であるから $(-1)^p = -1$

a^{p-k} ($1 \leq k \leq p-1$) は偶数であるから 2 で割り切れる --- (2)

$$pC_k = \frac{p!}{(p-k)!k!} = p \frac{(p-1)!}{(p-k)!k!}$$

p は素数より, $1 \leq k \leq p-1$ のとき, $(p-k)!k!$ は素因数に p を持たない
 ところで pC_k は整数であるから, $\frac{(p-1)!}{(p-k)!k!}$ は整数

よって pC_k は p で割り切れる --- (3)

①②③より題意は示された。

(ii) b が偶数のとき

$$a = (b+1)^p - b^p = \sum_{k=1}^p pC_k b^{p-k} = \sum_{k=1}^{p-1} pC_k b^{p-k} + 1 \quad \text{--- (4)}$$

b^{p-k} ($1 \leq k \leq p-1$) は偶数であるから 2 で割り切れる --- (5)

(i) と同様にして, pC_k は p で割り切れることがわかる --- (6)

④⑤⑥より題意は示された。